

TC2600

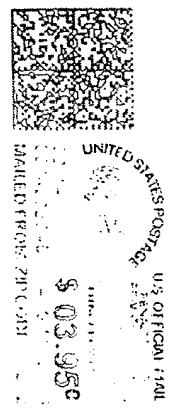
Bldg./Room

PNZ

Organization
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS
OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPLOYER

Handwritten signature



Handwritten mark



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,916	12/20/2000	Franciscus Lucas Antonius Johannes Kampferman	PHN 17,841	9592

7590 08/11/2004

PHILIPS ELECTRONICS NORTH AMERICAN CORP
580 WHITE PLAINS RD
TARRYTOWN, NY 10591

EXAMINER

BELIVEAU, SCOTT E

ART UNIT PAPER NUMBER

2614

DATE MAILED: 08/11/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED
AUG 17 2004
Technology Center 2600

Office Action Summary

Application No.

09/741,916

Applicant(s)

KAMPERMAN ET AL.

Examiner

Scott Beliveau

Art Unit

2614

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 December 2000 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1.4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Europe on 22 December 1999. It is noted, however, that applicant has not filed a certified copy of the EPO 99204469.3 application as required by 35 U.S.C. 119(b).

Specification

2. The disclosure is objected to because of the specification does not adhere to the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
- (e) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.
 - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (f) BRIEF SUMMARY OF THE INVENTION.
- (g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).

Art Unit: 2614

- (h) DETAILED DESCRIPTION OF THE INVENTION.
- (i) CLAIM OR CLAIMS (commencing on a separate sheet).
- (j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

3. The disclosure is objected to because the claim as written is grammatically incorrect. In particular, the recitation of "... in which access system a descrambler . . and means for storing entitlements are associated to the receiver, and in which access system if a match between the entitlement identification in the entitlement control message . . ." (IA: Page 1, Lines 6-9) is grammatically incorrect. Appropriate correction is required.

Information Disclosure Statement

4. The information disclosure statement filed 17 May 2001 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered unless otherwise indicated.

Drawings

5. The drawings are objected to because the Figure lacks labels for elements 2-10 which render it difficult to quickly ascertain the particular components. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the

Art Unit: 2614

immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency.

Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled “Replacement Sheet” in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

6. Claim 1 is objected to because the recitation of “ . . . in which access system a descrambler . . . and means for storing entitlements are associated to the receiver, and in which access system if a match between the entitlement identification in the entitlement control message . . . ” (Claim 1, Lines 5-8) is grammatically incorrect. Appropriate correction is required.
7. Claim 8 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite

Art Unit: 2614

the claim(s) in independent form. In particular, claim 8 appears to simply restate the limitations of the receiver of claim 1.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claim 1-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Coutrot et al. article (of record).

In consideration of claims 1 and 8, as set forth in the instant application (IA: Page 1, Lines 1-14), the Coutrot et al. article discloses the existence of “a conditional access system for controlling the access of receivers of end-users to data transmitted from a data content source in an uplink system, said uplink system comprising a scrambler for scrambling the content supplied from the content source, an entitlement control message generator for generating entitlement control messages containing a control word and an entitlement identification, and a transmitter for transmitted the scrambled content and the entitlement control messages, in which access system a descrambler, an entitlement control message decoder and means for storing entitlements are associated to the receiver, and in which access system if a match between the entitlement identification in the entitlement control message and the entitlement of the end-user exists, the entitlement control message decoder supplies a control word to the descrambler for descrambling a part of the received scrambled

content for which the receiver is entitled”. The Coutrot et al. article further discloses the particular method for facilitating entitlements in connection with the ordering/authorization PPV events wherein “meta-entitlement information includes an event number range” (Section 4.2 – Pay Per View) and may utilize prepaid tokens associated with pre-booked events (Section 2.2 – Management of Entitlements). The “receiver” subsequently comprises “means for extracting from the meta-entitlement an actual entitlement identification including the event selected by the end-user after which a control word from the entitlement control message is supplied to the descrambler if the entitlement identification in the entitlement control message matches the actual entitlement” (Section 6 – Information contained in Messages).

Claim 2 is rejected wherein the “meta-entitlement is transmitted in an entitlement management message to the entitled receiver” (Section 7 – Addressing Messages (EMMs)).

Claim 3 is rejected wherein the “actual entitlement is extracted from both the meta-entitlement and the entitlement control message” such that components from the both the EMM and the ECM are required to decrypt the program.

Claim 4 is rejected wherein the “meta-entitlement” further comprises a “data range” indicating its lifetime (Section 6.1 – Security Principles).

Claim 5 is rejected wherein the “meta-entitlement includes a number of allowed selections” (Section 4.2 – Pay Per View).

Claim 6 is rejected wherein the “receiver side” further comprises a “selection counter . . . set to the number of allowed selections in the meta-entitlement . . . and is decremented by each event election by the end-user (Section 4.2 Pay Per View).

Art Unit: 2614

Claim 7 is rejected wherein the “event number generator” is inherently either directly or indirectly “connected to the entitlement control message generator” by the very nature that both reside at the service provider.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as follows. Applicant is reminded that in amending in response to a rejection of claims, the patentable novelty must be clearly shown in view of the state of the art disclosed by the references cited and the objections made.

- The Wasilewski et al. (US Pat No. 6,157,719) reference discloses a cable television system and method for facilitating the delivery of entitlement management information wherein the entitlement information further comprises an event number range.
- The Bayassi et al. (WO 98/43426) reference discloses a digital television satellite system that facilitates the deliver of “meta-entitlement data” associated with pre-booked PPV events wherein such events are uniquely identified.
- The Candelore (US Pat No. 6,057,872) reference discloses a system and method for the delivery of “meta-entitlements” in the form of tokens facilitating the ordering of PPV events.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott Beliveau whose telephone number is 703-305-4907.

The examiner can normally be reached on Monday-Friday from 8:30 a.m. - 6:00 p.m..

Art Unit: 2614

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John W. Miller can be reached on 703-305-4795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SEB
July 27, 2004



JOHN MILLER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600

Notice of References Cited	Application/Control No. 09/741,916	Applicant(s)/Patent Under Reexamination KAMPERMAN ET AL.	
	Examiner Scott Beliveau	Art Unit 2614	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,057,872	05-2000	Candelore, Brant	725/23
	B	US-6,157,719	12-2000	Wasilewski et al.	380/210
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	WO 9843426 A1	10-1998	World Intellect	BAYASSI et al.	H04N 07/16
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



Form PTO-148
U.S. DEPARTMENT OF COMMERCE
(REV. 7-80) PATENT AND TRADEMARK OFFICE

Atty. Docket No.

PHN 17,841

Serial No.

09/741,916

Applicant

FRANCISCUS L. KAMPERMAN

Filing Date

DECEMBER 20, 2000

Group

2611

INFORMATION DISCLOSURE CITATION
(Use several sheets if necessary)

U.S. PATENT DOCUMENTS

Ex. Int.		Document Number	Date	Name	Class	Sub- class	Filing Date If Approp.
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Sub- class	Trans.
							Yes No
28	AG	0 1 2 8 5 5 5 A 2	12/1984	EUROPE	H04N	7/16	
	AH	W 0 9 9 0 7 1 5 1	2/1999	PCT (WORLD)	H04N	7/167	
	AI						
	AJ						
	AK						

OTHER (Including Author, Title, Date, Pertinent Pages, Etc.)


AL	
AM	
AN	

Examiner *hABh*

Date Considered 7/12/04

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with M 609; Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

Form PTO-1449 U.S. DEPARTMENT OF COMMERCE (REV. 7-80) PATENT AND TRADEMARK OFFICE				Atty. Docket No. PHN 17,840		Serial No.	
INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)				Applicant FRANCISCUS L.A.J. KAMPERMAN ET AL			
				Filing Date CONCURRENTLY		Group	

Jc945 U.S. PTO
 09/741916

 12/20/00

U.S. PATENT DOCUMENTS												
Ex. Int.	AA	AB	AC	AD	AE	AF	Document Number	Date	Name	Class	Sub-class	Filing Date If Approp.

FOREIGN PATENT DOCUMENTS														
								Document Number	Date	Country	Class	Sub-class	Trans.	
													Yes	No

OTHER (Including Author, Title, Date, Pertinent Pages, Etc.)														
✱	AL	Coutrot et al., "A Single Conditional Access System for Satellite-Cable and Terrestrial TV", IEEE Transactions on Consumer Electronics, vol. 35, no. 3, Aug. 1998, pp. 464-468												
	AM													
	AN													

Examiner <i>hth</i>	Date Considered 7/12/04
---------------------	-------------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP Draw line through citation if not in conformance and not considered. Include a copy this form with next communication to applicant.



US006057872A

United States Patent [19]
Candelore

[11] **Patent Number:** **6,057,872**
 [45] **Date of Patent:** **May 2, 2000**

[54] **DIGITAL COUPONS FOR PAY TELEVISIONS**

0 833 511 4/1998 European Pat. Off. .
 WO 96/32702 10/1996 WIPO .

[75] **Inventor:** **Brant Candelore, San Diego, Calif.**

[73] **Assignee:** **General Instrument Corporation,**
Horsham, Pa.

Primary Examiner—Nathan Flynn
Attorney, Agent, or Firm—Barry R. Lipsitz; Ralph F. Hoppin

[21] **Appl. No.:** **08/890,066**

[22] **Filed:** **Jul. 9, 1997**

[51] **Int. Cl.**⁷ **H04N 7/10**

[52] **U.S. Cl.** **348/3; 348/10**

[58] **Field of Search** **709/217-219;**
345/327, 328; 348/6, 7, 8, 3, 1, 10, 12,
13, 2; 455/4.1, 4.2, 5.1, 52; H04N 7/10

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,876,592 10/1989 Von Kohorn .
 5,128,752 7/1992 Von Kohorn .
 5,249,044 9/1993 Von Kohorn .
 5,260,778 11/1993 Kauffman et al. .
 5,532,735 7/1996 Blahut et al. 348/13
 5,604,542 2/1997 Dedrick .
 5,610,653 3/1997 Abecassis 348/110
 5,838,314 11/1998 Neel et al. 345/327

FOREIGN PATENT DOCUMENTS

0 656 728 6/1995 European Pat. Off. .

51 Claims, 7 Drawing Sheets

[57] **ABSTRACT**

Digital coupons are selectively transmitted in a communication network to subscriber terminals for promotional purposes. Subscribers automatically receive coupon credits when they meet the preconditions of the digital coupons. Free or reduced price pay-per-view (PPV) programming in particular may be provided when a subscriber purchases a given number of PPV programs at a regular price. The terminals maintain a running balance of available coupon credits and inform the subscriber via a user interface of the available balance. Subscribers can be rewarded for viewing commercial messages by awarding coupons which can be immediately redeemed for PPV programs. With an optional report back capability, terminal usage pattern data can be retrieved and analyzed by program service providers to determine the effectiveness of the promotions and to gather additional demographic and individual data. The integrity of the scheme is assured with encryption techniques.

400

410 YOU ARE NOT SUBSCRIBED TO THE PROGRAM.
 420 HOW DO YOU WISH TO VIEW THE MOVIE?
 430 YOUR OPTIONS ARE:
 440 a)IMPULSE PAY-PER-VIEW
 -THE COST IS \$3.50 FOR THE MOVIE.
 -YOU HAVE \$27.50 CREDIT.
 450 b)COUPONS
 -THE COST IS 7 TV COUPONS.
 -YOU HAVE 13 TV COUPONS.
 460 a)IMPULSE PAY-PER-VIEW WITH DISCOUNT
 -THE COST IS \$1.50 WITH 4 TV COUPONS.
 -YOU HAVE \$27.50 CREDIT AND
 13 TV COUPONS.

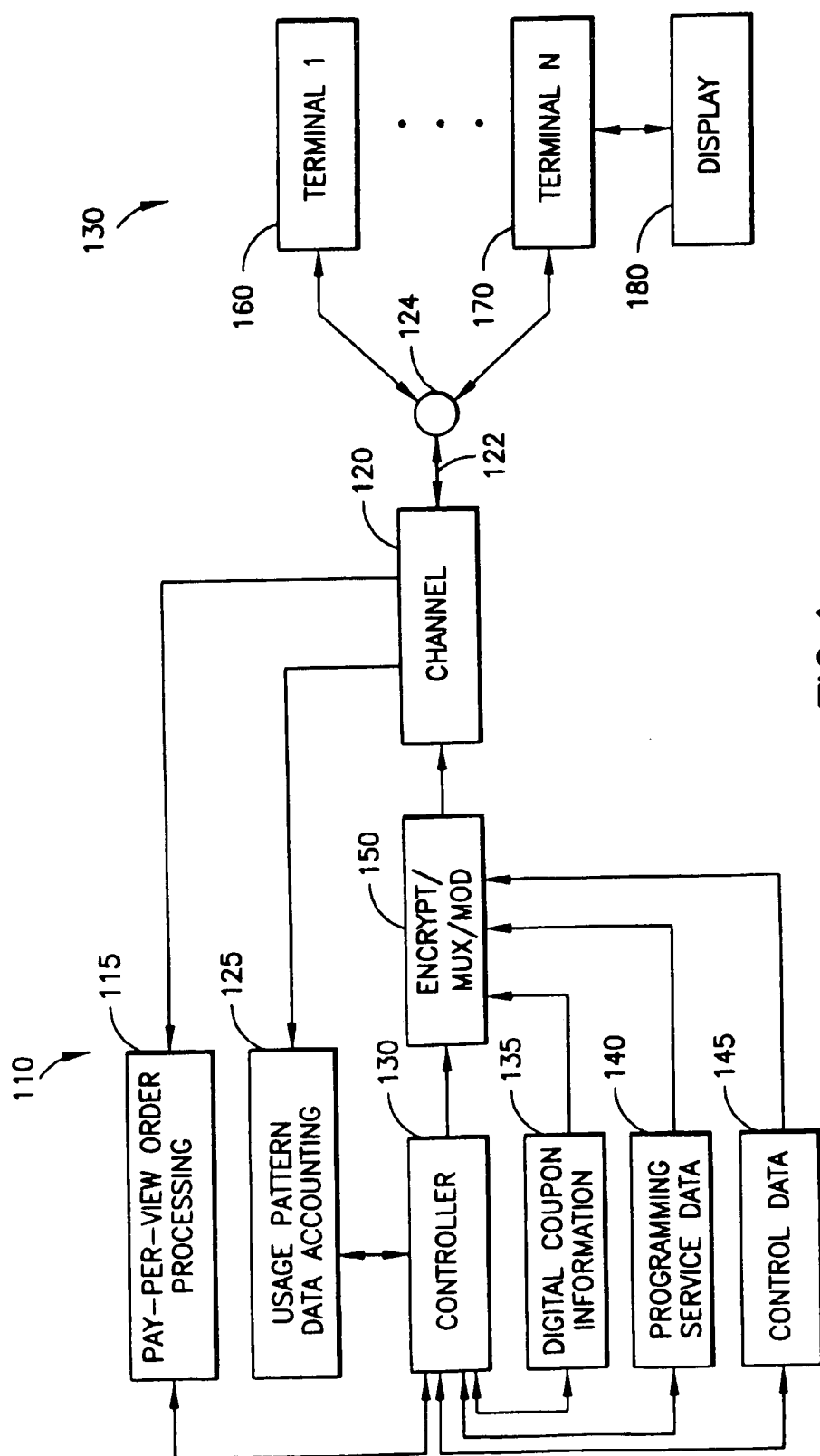


FIG. 1

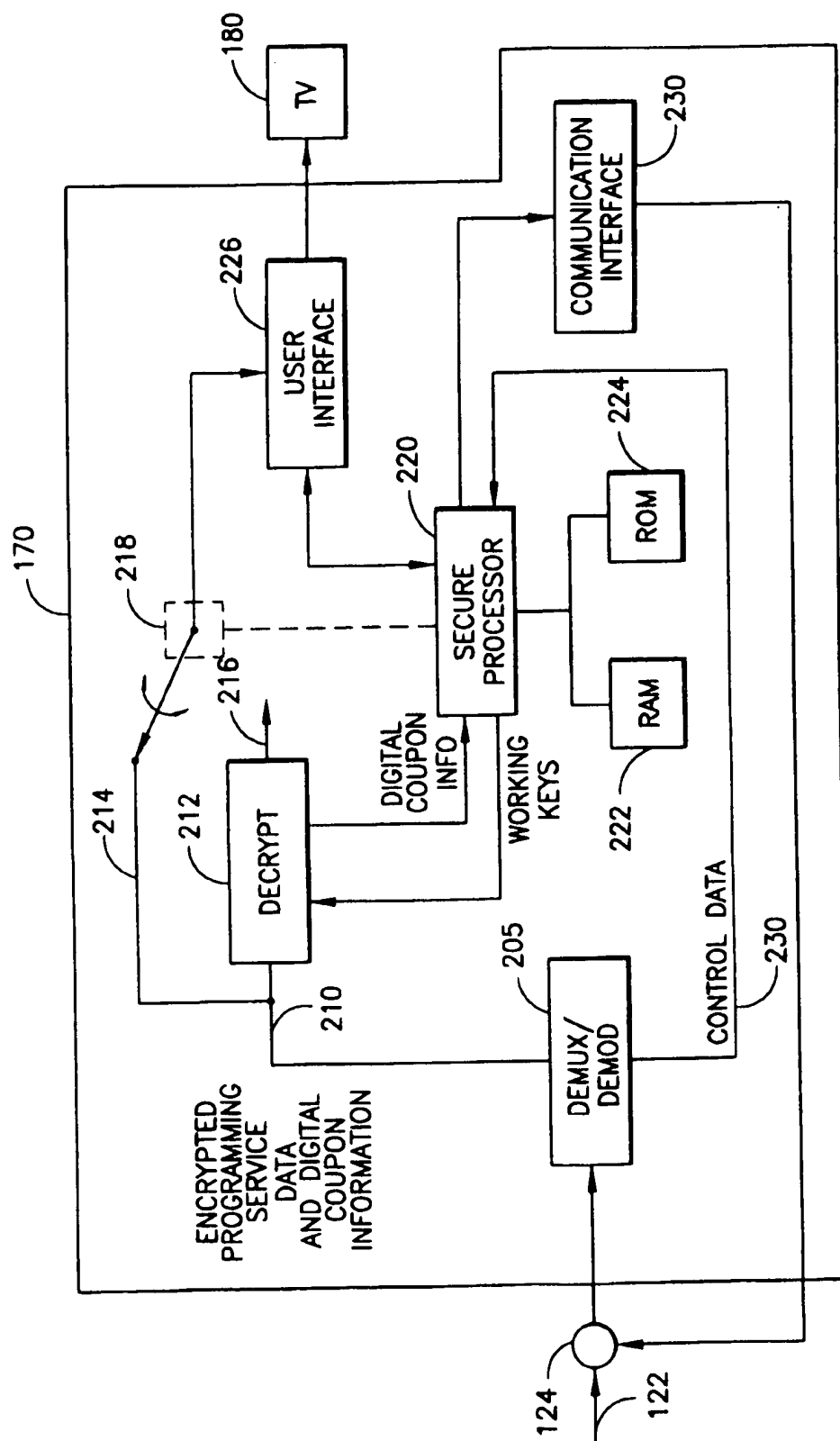


FIG. 2

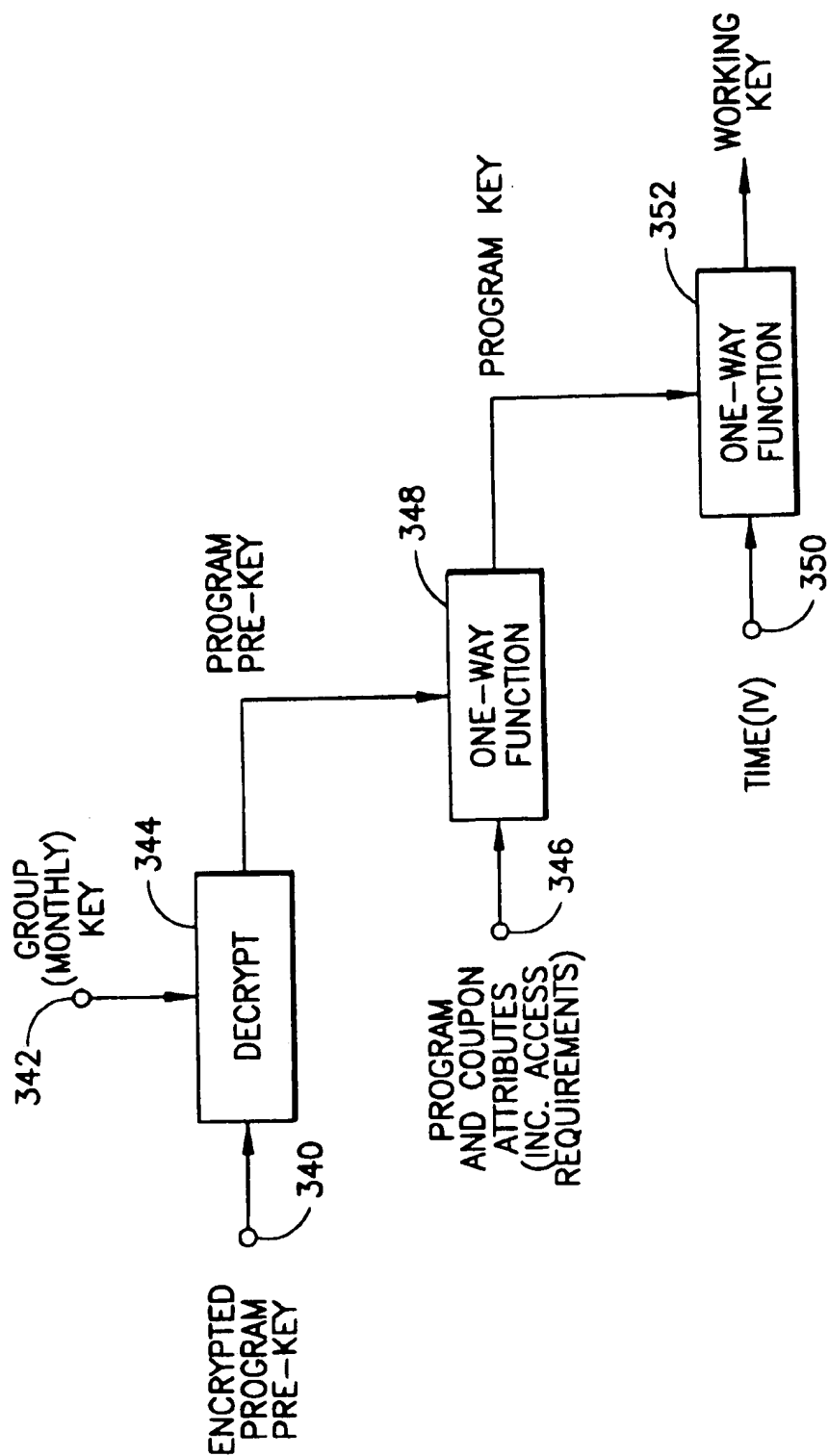


FIG. 3

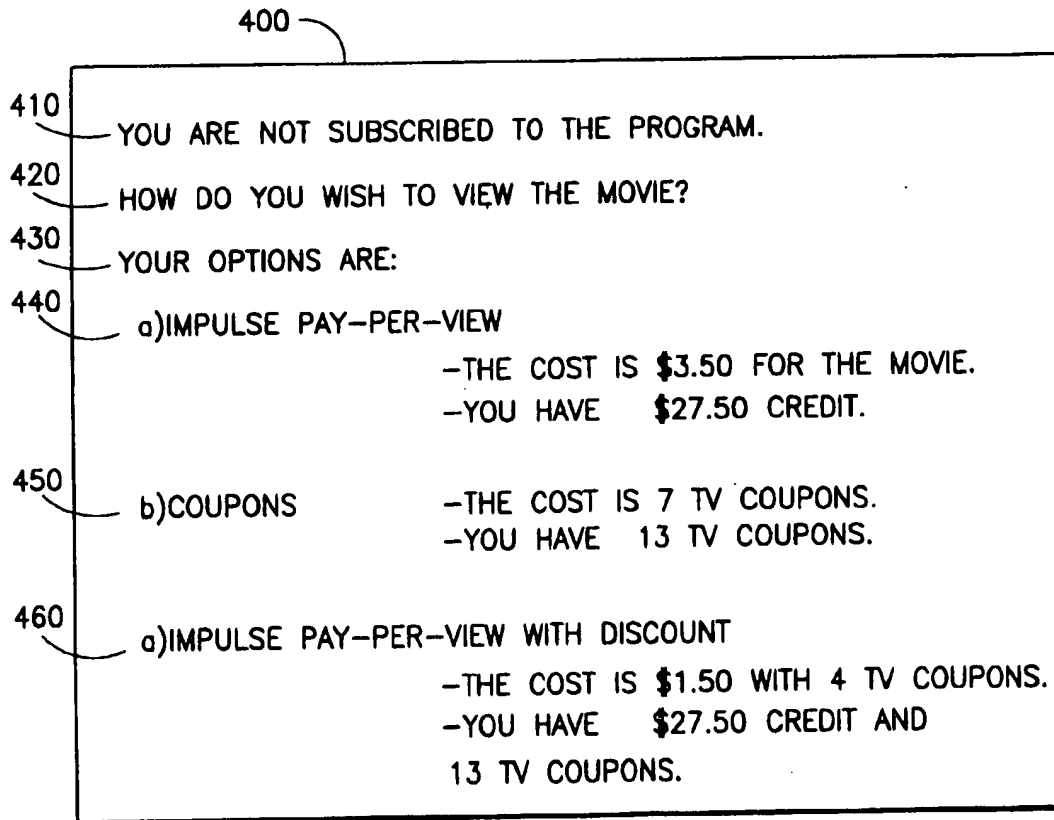


FIG.4

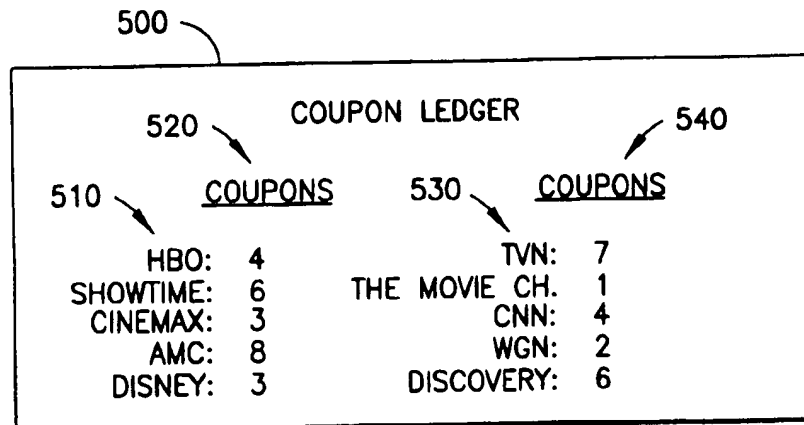


FIG.5

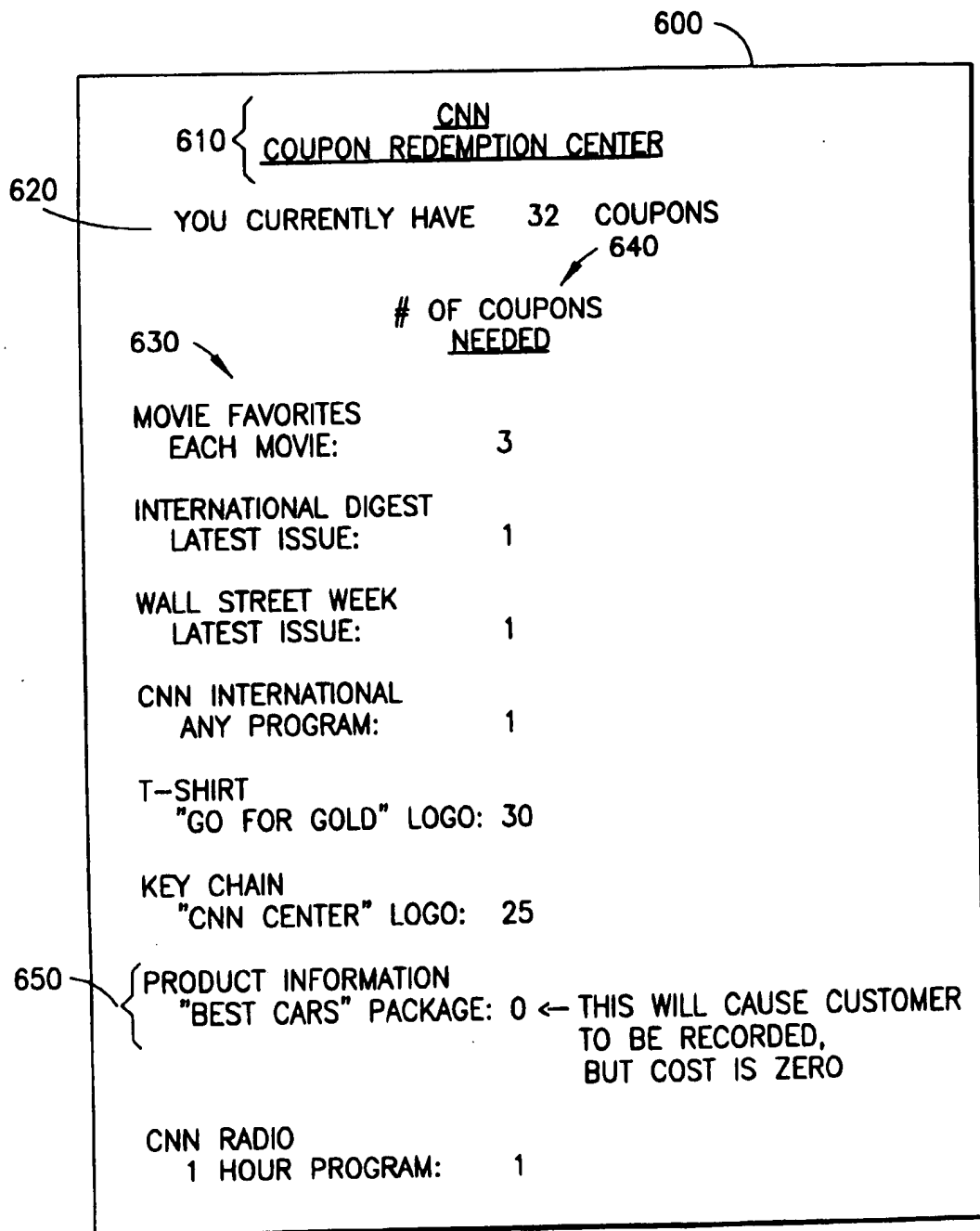
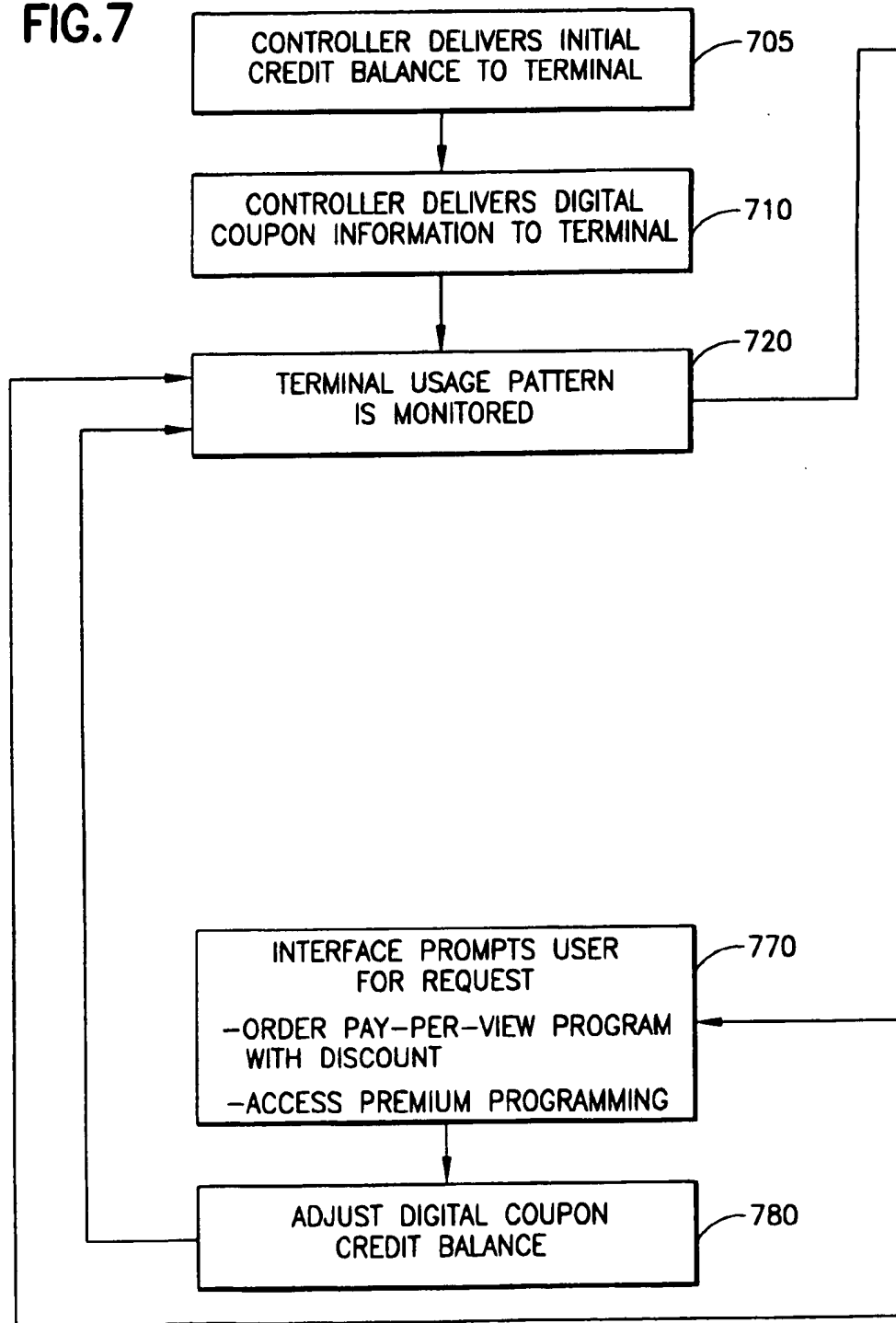


FIG.6

FIG.7A **FIG.7B****FIG.7****FIG.7A**

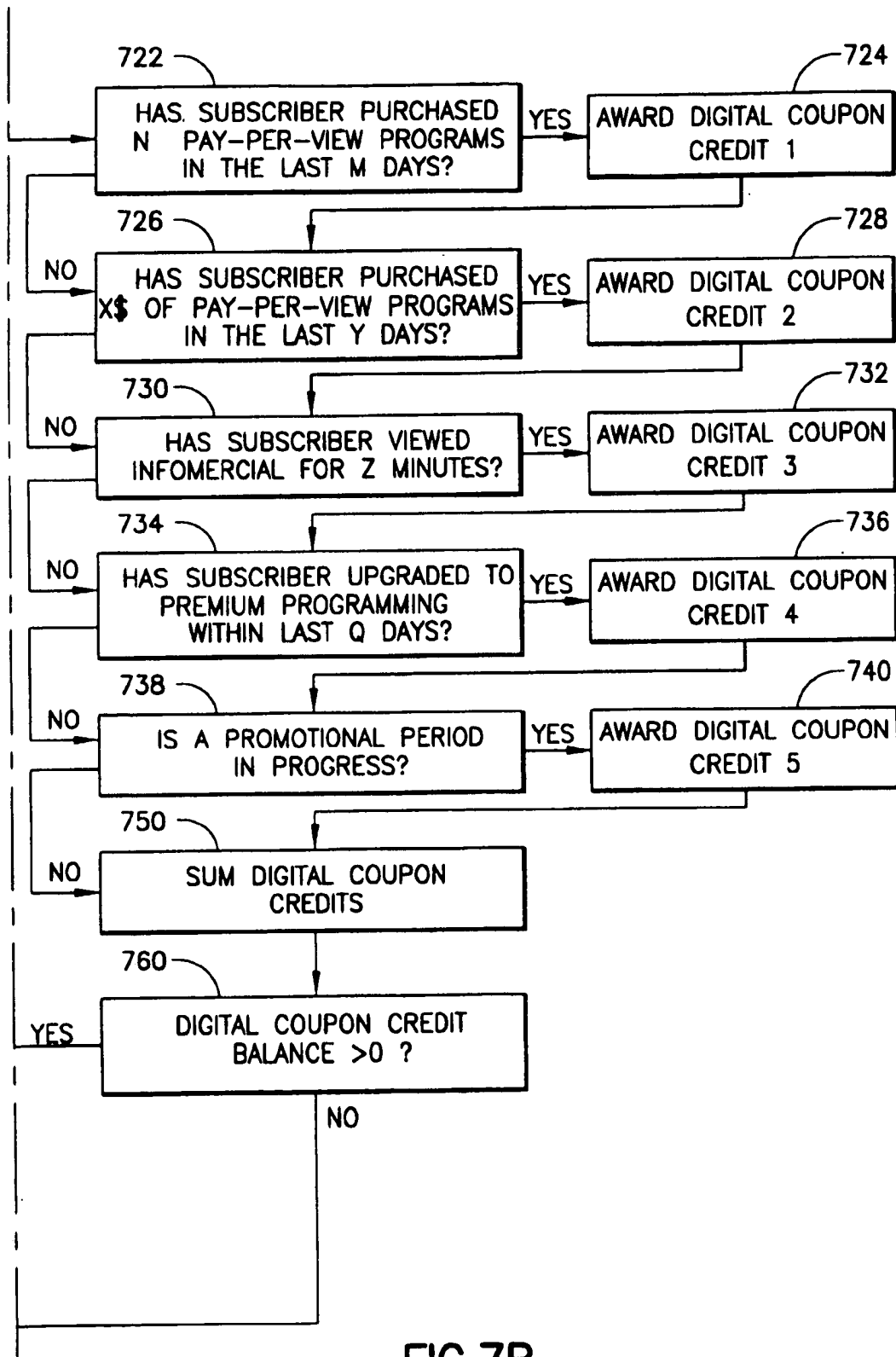


FIG.7B

DIGITAL COUPONS FOR PAY TELEVISIONS**BACKGROUND OF THE INVENTION**

The present invention relates to communications networks such as cable television, satellite television and computer networks over which services are available for a fee. In particular, an apparatus and method are presented for allowing users of services such as pay television to obtain credits when viewing particular programs. The invention enables service providers to transmit credit information in the form of "digital coupons" to individual subscriber terminals to promote particular programs and reward viewer loyalty.

Cable and satellite television networks where video services are available for a fee are well known. Also well known are computer network services such as CompuServe, Prodigy, America Online, Knight-Ridder Information Service, and others where databases, banking and shopping services can be accessed and e-mail and the like can be communicated, all for a fee. In the past, some networks have provided services on a free trial basis. For example, during promotional periods lasting for one or two days, premium programming services such as movie or sports channels could be viewed by subscribers who normally would have to pay an additional charge to receive such programming. In most cases, this is done by placing the entire service into some sort of promotional scrambling mode where the programs are either not scrambled, i.e. in-the-clear, or use fixed keys which are known to all subscriber terminals. For example, in a broadcast environment, service providers do not know which existing customer or potential new customer is attempting to access a particular service. Even if feedback could be obtained, for example, using a telephone line or some upstream path, there would be too many transactions of customers tuning in and out of services for the service provider to usefully analyze.

Consequently, the service must usually be placed in a scrambling mode which allows free access by everyone, including potential new customers and even existing customers, or at least a large defined group. Moreover, an extended period of free service time is usually needed to effectively promote services since the different programs which are made available during the free preview will appeal to different interest, demographic, and age groups of viewers. For example, some viewers may prefer to see action movies while others prefer to see comedies. Thus, it is necessary to provide a wide variety of free programming over an extended period of time to effectively encourage viewers to subscribe to the premium programming services for an additional monthly charge.

During the free preview period, renewal and new subscriptions rates may be reduced to further motivate the customer since the customer may otherwise wait until after the free preview period is over to order new services which may, in turn, stress the call handling capability of the service provider's subscription center.

Additionally, various programs may be offered on an individual or a-la-carte pay-per-view (PPV) basis, where the subscriber pays a fee to view a single program. The customer may either call ahead to the subscription center to have a specific authorization or entitlement for a single program sent to the customer's terminal, or the customer can arrange to have a certain amount of monetary credit downloaded into the customer's terminal. With the selection of PPV program, the pre-stored credit amount in the terminal is reduced. Such PPV may be offered at fixed times or staggered times with

so-called Near Video On Demand (NVOD). Also programs may be delivered essentially instantaneously with Video On Demand (VOD).

In VOD system systems, the program can be delivered on demand to a specific subscriber when that subscriber communicates a buy signal to a video server located at a cable television system headend. The buy signal may be communicated, for example, through an available upstream channel in a cable television network, or via a telephone line.

Various marketing techniques have been used to encourage subscribers to purchase pay-per-view programs. PPV usually are more profitable for the service provider than subscription services. These marketing techniques include providing the subscriber with a credit on his monthly statement when the subscriber purchases a predetermined number of PPV programs, or spends a predetermined amount of money on PPV programs. Or, the subscriber may be mailed a paper coupon which the subscriber can later mail back to the network billing department to obtain a discount after the subscriber has met the preconditions for redeeming the coupon. For example, the paper coupon may entitle the subscriber to a credit of one-half the price of a PPV program when one PPV program is purchased at the regular price.

While such marketing techniques can be effective, some subscribers may become accustomed to receiving paper coupons and other discounts on their monthly statements and may then resist paying higher fees when such discounts are not offered. In other words, they will only buy if they get a coupon. It would be desirable to reward the subscribers after they have met some predetermined conditions. Additionally, it is not easy to selectively target groups of subscribers or individual subscribers, without making the entire service free, or to monitor the effectiveness of such promotions. Moreover, the effectiveness of conventional promotions may be reduced because the realization of the discount by the subscriber is delayed, typically for a number of weeks due to delays in the billing cycle. Furthermore, paper coupons are difficult to organize and handle and are easily lost.

Accordingly, it would be desirable to provide a method and apparatus for allowing selective targeting of promotions of programming services to particular subscribers or groups of subscribers without placing services in free mode, or using paper coupons. The system should allow subscribers to receive an immediate credit when a predetermined viewing pattern has been met. The system should reward subscriber loyalty and encourage subscribers to purchase additional programming services such as PPV programs and/or additional levels of service, such as premium programming services.

The system should also organize the credits in a way to allow the subscriber to take a quick inventory, and should inform the subscriber when a service is available through the promotion. The system should allow flexibility as to how the credits may be used, for example, in regard to the variety of shows, times, and dates the programming may be accessed.

Furthermore, it would be desirable to provide a system for monitoring the success of such promotions, gain feedback on subscriber viewing habits, and determine the viewership (e.g., audience size) of particular programs. The system should employ cryptographic techniques to thwart unauthorized persons (e.g., pirates) who attempt to tamper with the system for illicit gain.

The present invention provides a system having the above and other advantages.

SUMMARY OF THE INVENTION

In accordance with the present invention, an apparatus and method are presented for allowing users of services such

as pay television to obtain credits when viewing particular programs. The invention enables program service providers to transmit credit information in the form of "digital coupons" to individual subscriber terminals to promote particular programs and reward viewer loyalty.

A communication system in accordance with the present invention includes a controller for transmitting program services to a plurality of subscriber terminals via a communication channel. The program service may include television programs which are broadcast or continuously transmitted on a predetermined schedule, pay-per-view programs which require specific user selection and either a local transacted or remotely transacted purchase, Near Video-On-Demand which is pay-per-view offered at staggered broadcast times, and Video-On-Demand services, which are transmitted only in response to a user request, or other electronic information such as computer software.

The communication channel may include a cable plant and/or satellite link, for example. The program services can be selectively recovered by the subscriber terminals. For example, a subscriber may select a particular program to view by tuning in the corresponding channel using an on-screen interface, e.g. Electronic Program Guide (EPG), and a remote control unit, or by transmitting a buy order for either PPV or Video-On-Demand programming.

The controller can deliver digital coupon information to the terminals along with program service data using any available technique, such as frequency or time multiplexing. The digital coupon information allows the terminals to obtain credits when recovering particular programs as defined by preconditions of the digital coupon information. For example, the subscriber may receive a credit for one free PPV program when the precondition of purchasing five PPV programs at regular prices has been met. The terminal automatically tracks the balance of coupon credits as coupons are awarded and redeemed. The credits are usable in obtaining program services at a reduced charge (e.g., at a discount or free).

Each terminal includes a processor which monitors a usage pattern (e.g., viewing history) of the terminal to determine if the preconditions of the digital coupon information have been satisfied. For example, the usage pattern may indicate which programs have been recovered by the terminal within the last month, or some other period, or the length of time that a particular program, or program service (e.g., channel) was viewed. The terminal may simply grant coupons based on the purchase of a PPV program, or based on the amount of time spent viewing an infomercial. The credits are thus awarded when there is a correlation between the usage pattern and the preconditions of the digital coupon information.

A user interface such as a graphical user interface (e.g., on-screen display) may be provided to allow the subscriber to selectively redeem the credits. For example, the user may have a variety of options from which to choose, where a cash balance and/or a coupon balance are redeemed in full or in part. The user interface can also be used to obtain a confirmation of user involvement. For example, to verify that the subscriber is still viewing a program, he may be periodically required to provide some sort of control input as the program is displayed.

When the program services include individual programs which can be individually recovered by the terminals, such as with a PPV scheme, the coupon credits are awarded when the usage pattern indicates that a terminal has recovered a particular number of such individual programs, or a particu-

lar amount of charges. This allows a coupon credit to be awarded whenever a PPV program has been accessed. One or more coupons may need to be redeemed in order to access a program.

To allow program service providers and advertisers to obtain and analyze the terminal usage data, a usage pattern accounting center which is associated with a network controller may be provided. The usage pattern accounting center can receive usage pattern data from the terminals via a communication link, such as an upstream path in the channel over which the program services are transmitted, or a telephone network. This is especially useful for determining the viewership of commercials or infomercials wherein the cost of running the ad in a program is oftentimes a function of the estimated viewing audience.

Moreover, the network controller can control the delivery of the digital coupon information to the terminals based on the received usage pattern data. In this case, the network controller can deliver the digital coupons directly to the terminal in a similar fashion as with other entitlements such as subscription entitlements, PPV entitlements, and credit information. For example, subscribers who demonstrate a preference for sports programs can receive digital coupon information which provides discounts for future special sports events.

The controller can thus deliver different digital coupon information to the different subscriber terminals based on the usage pattern data or other demographic or individual data which has been compiled by other means. The digital coupon information can provide different preconditions for obtaining the same credits, or the same preconditions for obtaining different credits. For example, it is possible to reward favored subscribers such as those who purchase relatively more programming by providing the favored subscribers with more coupons than other, less favored, subscribers when the same viewing preconditions are met.

Various cryptographic techniques may also be employed to prevent unauthorized access to the digital coupons.

A corresponding subscriber terminal and method are also presented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a communication system in accordance with the present invention.

FIG. 2 is a block diagram of a subscriber terminal in accordance with the present invention.

FIG. 3 is a block diagram illustrating a decryption hierarchy for use in accordance with the present invention.

FIG. 4 is an on-screen display for a user interface in accordance with the present invention.

FIG. 5 is another on-screen display for a user interface in accordance with the present invention.

FIG. 6 is yet another on-screen display for a user interface in accordance with the present invention.

FIG. 7 is a flowchart illustrating a method for providing digital coupons in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A method and apparatus are presented for allowing users of program services such as pay television to obtain credits when viewing particular programs. The invention enables program service providers to transmit credit information in the form of "digital coupons" to individual subscriber ter-

minals to promote particular programs and reward viewer loyalty. The digital coupons may be generated locally in the terminals based on criteria sent by the service providers, or transmitted directly as an entitlement by the service provider.

FIG. 1 is a block diagram of a communication system in accordance with the present invention. The system includes a transmitting end, shown generally at 110, a channel 120, and a receiving end, shown generally at 130. The transmitting end 110 includes a central controller 130 which communicates with a PPV order processing function 115, a terminal usage pattern data accounting function 125, an encryptor/multiplexer/modulator 150, a digital coupon information function 135, a program service data function 140, and a control data function 145.

The receiving end 130 includes a number of terminals including terminal 1 (160) through terminal N (170), which receive the digital coupon information, program service data, and control data via a hub 124 and path 122. Each terminal has an associated display such as a television for displaying the program service data. For example, "terminal N" 170 has an associated display 180. In the example shown, the terminals 160, . . . , 170 are able to communicate with the PPV order processing function 115 and usage pattern data accounting function 125 via the channel 120.

For example, in a cable television network, such upstream communication may be provided on a channel (e.g., RF spectrum) which is separate from the channels over which the program service data is communicated. A frequency-division multiplexing scheme may be used to achieve this goal. Alternately, a time-division multiplexing scheme may be used, or the terminals 160, . . . , 170 may communicate with the PPV order processing function 115 and usage pattern data accounting function 125 via a separate communication link such as a telephone network. Moreover, as discussed in greater detail below, the present invention can be implemented without the PPV order processing function 115 and/or usage pattern data accounting function 125.

The channel 120 may comprise coaxial cable, optical fiber, and/or a wireless link such as a satellite or RF broadcast link. The transmitting end 110 of the system may be a cable television system headend, a satellite uplink center, or an RF broadcast center, for example.

The digital coupon information function 135 comprises a memory for storing digital coupon information in accordance with the present invention. The digital coupon information is communicated to the terminals 160, . . . , 170 at the receiving end 130 of the system. Furthermore, when the terminals 160, . . . , 170 are addressable, the digital coupon information may be targeted to individual terminals and/or to groups of terminals, for example, according to demographic data. Alternatively, the digital coupon information may be transmitted via a path which is separate from that of the program services.

The digital coupon information provides credits which the terminals can use for a number of purposes. For example, the digital coupon information may provide a discount when the terminals order one or more PPV programs through the PPV order processing function 115. As an example, if a terminal orders five PPV programs within the current billing cycle, the digital coupon credit may allow the terminal to order a sixth PPV program at no charge. Or, for terminals that order PPV programs infrequently, the digital coupon credit may allow the terminal to order a first PPV program at half-price. The digital coupon may be generated automatically based on program coupon criteria established by the service provider.

This has the advantage of requiring no direct involvement by the service provider. This is also suitable for broadcast environments where the return path either does not exist, is slow, or not set-up for interactive transactions.

Alternatively, the digital coupon information may allow the terminals to access premium program services at a reduced charge, or at no charge, or allow the terminals to access other information, such as a software program, a computer game, a book in electronic form, a musical composition, an on-screen television program guide, movie or restaurant reviews, or other promotional, informational or educational material. For example, the digital coupon information may allow a terminal to access a premium movie channel for two days with each PPV purchase, or to download one computer video game, or to gain one hour of free connect time to a computer database.

The term "program service" is thus used herein to encompass television, multimedia, and other audio and/or video signals as well as computer software or virtually any other information that can be accessed by, and/or communicated to, the terminals via the channel 120. The term "credit" is used herein to indicate that the terminals are provided with a benefit such as a reduced or waived charge when accessing and/or obtaining program services via the channel, or for obtaining merchandise via the channel which is delivered to the subscriber by other means (e.g., by mail).

The terminals 160, . . . , 170 do not realize the credit which is offered with the digital coupon information until the terminals satisfy certain preconditions. Each terminal includes means for monitoring various factors which define the terminal's usage pattern data over a defined time period, including, for example, the number of PPV programs purchased, the amount of PPV charges incurred, whether, and for what duration, the terminal has been tuned to a particular program or program service, whether the terminal has recently upgraded to one or more premium program services, and whether a promotional period is in effect. The promotional period may apply to individual terminals, such as those of new subscribers, to selected groups of terminals, or to all terminals.

Accordingly, monitoring means in the terminals monitor the above factors to determine whether the usage pattern of the terminal corresponds with the preconditions of the digital coupon information. Optionally, in a "report-back" function, the usage pattern data is periodically transmitted from the terminals to the usage pattern data accounting function 125, for example, via the hub 124 and channel 120, or, alternatively, via a telephone network. For example, the usage data may be transmitted daily, weekly, or monthly.

Such usage pattern data provides valuable information for program service providers and advertisers which can be used to better target individual subscribers and groups of subscribers with products and services with which they are likely to be interested. Moreover, the usage pattern data allows the interested parties (e.g., promoters and advertisers) to determine the effectiveness of various promotions. For example, when the digital coupon information provides a one-half price PPV program to subscribers who infrequently order PPV, the success rate of the program can be determined from the usage pattern data at the function 125.

As another example, when the digital coupon information provides two free days of access to one of a number of available premium program services, the selected premium program service can be monitored, and the subscriber can be subsequently offered a digital coupon which allows him to upgrade to the selected premium program service, e.g., at

one-half off the normal charge for the first month. Various other marketing strategies may be used with the present invention to enhance revenue and customer goodwill. For example, a subscriber may be given coupon credit for a free pay-per view movie on his birthday.

Moreover, the digital coupon balance may be adjusted according to lotteries or other contests or games. For example, subscribers may be able to enter a lottery for additional coupons if they spend a certain amount of money. Or, the subscriber may play interactive games of chance where the prizes and losses are determined in terms of coupons.

However, even if the usage pattern data is not reported back to the function 125, the monitoring means in the terminal can determine whether the usage pattern data meets the preconditions of the digital coupon information. Preferably, this is done in a secure manner to prevent tampering by pirates, as discussed in further detail below.

The controller 130 causes the digital coupon information from function 135 to be encrypted and multiplexed at the encryptor/mux/modulator 150 along with the program service data from function 140 and the control data from function 145. The program service data may comprise video and/or audio data which is stored locally on storage media, and/or which is received from an external source such as a satellite downlink. Alternatively, the program service data may comprise computer software or other electronic information.

The control data includes cryptographic data which is used for generating working keys at the terminals for decoding the received data. Typically, one or more premium program services are communicated with basic program services over the channel 120. Both the basic and premium program services may be accessed with possession of the appropriate group key or keys. The group key or keys are delivered as part of an Entitlement Management Message (EMM). Possession of the group key or keys along with the appropriate entitlement control data allows the terminals to recover program keys from the program data sent by the service provider in Entitlement Control Messages (ECM).

The program keys allow the derivation or decryption of the working keys which are used to encrypt the programming signal at the uplink or headend side, and to decrypt the program signals on the downlink or consumer decoder side. The term "recover" is used herein to indicate that a program service is received at a terminal and retrieved for use (e.g., display) by the subscriber.

The control data included in an Entitlement Control Message (ECM) is used to control access to a particular program service (i.e., channel). The ECM control data tells the terminal which entitlement needs to be held by the terminal in order to be authorized to access and recover the particular program service. Typically, the ECM message which delivers the control data information is also used to deliver the program key information. The ECM message therefore not only defines program parameters but also delivers a key or precursor key (e.g., pre-key).

The ECM control data may further include data for providing the terminals with the cost for ordering a PPV program. This control data may further indicate the cost, in terms of the number, and type of coupons required to access the program, along with other details listing what number of coupons is required for a discount, and so forth.

FIG. 2 is a block diagram of a subscriber terminal in accordance with the present invention. Like-numbered elements correspond to the elements of FIG. 1. A

demultiplexer/demodulator 205 of the terminal 170 receives the program service data, digital coupon information, and control data from the path 122 and hub 124. Demultiplexing and demodulating is performed using conventional techniques. The encrypted program service data is provided to a decryption processor 212 and a switch 218 via lines 210 and 214, respectively, while the encrypted control data and digital coupon information are provided to a secure processor 220 via line 230.

The encrypted program service is decrypted by the decryption processor 212 to provide a clear signal at output 216 of the decryption processor. The secure processor 220 may receive the decrypted digital coupon information from the decryption processor 212. The decryption processor 212 can utilize a conventional decryption scheme, such as that disclosed in Gilhousen, et al., U.S. Pat. No. 4,613,901 entitled "Signal Encryption and Distribution System for Controlling Scrambling and Selective Remote Descrambling of Television Signals," or Bennett et al., U.S. Pat. No. 4,864,615 entitled "Reproduction of Secure Keys By Using Distributed Key Generation Data," both incorporated herein by reference.

The decryption processor requires working keys (WK) to decrypt the signals input thereto via line 210. The working keys are generated by the secure processor 220 in response to the control signals received via line 230. Firmware for the secure processor is stored in read only memory (ROM) 224. The secure processor 220 is also provided with random access memory (RAM) 222. A secure portion of the RAM 222 holds unit specific keys and/or seeds for use in decryption of a monthly group key, as discussed in greater detail in connection with FIG. 3.

A user interface 226 enables a viewer to select program services for viewing on a television (TV) 180. If a user is authorized to receive the selected service by subscription, individual purchase (e.g., pay per view), or according to a digital coupon credit, the secure processor 220 will actuate the switch 218 to couple the decrypted output 216 from decryption processor 212 to the TV 180 via user interface 226. Otherwise, the user interface and TV will only receive the encrypted signal via line 214 and switch 218. As will be appreciated by those skilled in the art, switch 218 could alternatively be configured to provide a Barker channel (e.g., a fixed message) to the user, or no signal at all, in the event that the user is not authorized to access the selected service.

The secure processor 220 monitors the programming which is selected by the user via the user interface 226 to determine whether the user has met the preconditions for obtaining the digital coupon credit. For example, if the digital coupon provides a credit for one free PPV program when five PPV programs are purchased at the regular price, the secure processor will record each occurrence of a purchase of a PPV program. The RAM 222 may be used to store the corresponding data. The usage pattern data thus includes data which is related to the digital coupon preconditions but can include other user selections as well. A communication interface 230 such as a data modem is provided to allow the terminal to transmit buy orders for VOD programming and certain types of programming which require a service provider's authorization for acquisition to the PPV order processing function 115 of FIG. 1. PPV purchases processed locally by the terminal and stored internally to the terminal may be forwarded to the PPV processing function for billing purposes. The interface 230 also allows the terminal 170 to transmit the usage pattern data to the usage pattern data accounting function 125 of FIG. 1.

The terminal receives control data in the form of an Entitlement Management Message (EMM) which provides

an initial currency credit balance for the terminal 170. In this case, when a user orders PPV programs, for example, the overall currency credit balance is decreased by the cost of the programs. The EMM message originating from the service provider may or may not deliver an initial or additional coupon credit to the terminal.

Typically, coupon credit is generated when the preconditions for obtaining the digital coupon credit are realized. The coupon credit balance can be immediately adjusted. As an illustration, assume the initial credit balance is \$40, and each PPV program costs \$5. Then, the credit balance will drop successively to \$35, \$30, \$25, \$20 and \$15 after the first five programs are purchased. At this time, the usage pattern data meets the preconditions of the digital coupon information, and the coupon credit balance gets incremented by one.

Alternatively, the coupon credit balance is incremented by one with each PPV purchase. When the terminal tunes in to the sixth program, the terminal receives a Entitlement Control Message (ECM) for the program. The terminal uses the ECM to determine the different ways that the program may be accessed. The ECM will also describe the currency cost and the coupon cost, if the program is available by coupon. The terminal will automatically determine whether or not the terminal has a coupon or coupons to acquire the program. If so, the program is automatically offered to the viewer, or the viewer is prompted to purchase the program using currency or coupons.

By choosing the coupon option, the next order for a PPV program is provided free, and the coupon credit field is decremented appropriately. Thus, the balance remains at \$15. Alternatively, the terminal is charged for the sixth program, but the secure processor increments the credit balance by the cost, so there is no net change in the credit balance. The secure processor may provide a display on the user interface 226 that informs the viewer that the preconditions of the digital coupon information have been met. Of course, it is possible for coupon credits to accumulate when the corresponding preconditions are met but the credits are not realized, i.e., cashed in. The credits may be retained at the terminal for a predetermined period such as two or three months, or indefinitely. The secure processor may inform the subscriber if the credits are about to expire.

As described in further detail below in connection with FIGS. 4-6, the viewer may query the user interface 226 to determine the credit balance along with other related information.

FIG. 3 is a block diagram illustrating a decryption hierarchy for use in accordance with the present invention. An encrypted program pre-key is input via terminal 340 to a decryption function 344 which also receives a monthly group key via terminal 342. The program pre-key is unique to each encrypted program offering (e.g., television program) that is available for decryption. The group key is changed on a periodic basis, e.g., once each month. The decryption function 344 decrypts the encrypted program pre-key to provide a program pre-key that is used as one input to a one-way function 348. The other input to one way function 348 comprises various program and coupon attributes, including access requirements, such as coupon and currency cost, for the corresponding program. The access requirements must be met to obtain authorization to view the program. The program and coupon attributes are input via terminal 346, and the one way function processes the program pre-key and program attributes to provide a program key.

The program key output from one way function 348 is used as one input to another one way function 352 that also

receives, via terminal 350, an initialization vector (IV) representative of time. The processing of the initialization vector and program key by one way function 352 generates the working keys required by decryption processor 212 of FIG. 2 to decrypt the program service selected by an authorized user. A further description of the generation of the various keys, including working keys (provided in a "keystream"), can be found in the aforementioned Bennett, et al. patent.

Optionally, the digital coupon information and program services can be encrypted according to a common cryptographic key. This could allow an authenticated file, for example, which represents a coupon image, to be sent to the decoders. The coupon could subsequently be redeemed as an authenticated image by transmitting the coupon from the decoder to the program service provider or other accounting center.

FIG. 4 is an on-screen display for a user interface in accordance with the present invention. The display 400 may be invoked as part of a graphical user interface (GUI) which allows a user to select channels and control other features such as volume and the like. Such interfaces are well known in the art. The display 400 may be controlled by a hand-held remote control, a pointing device, voice command or any other available means. For example, a user may select a PPV program such as a movie from a graphical user interface which causes the display 400 to appear.

The display 400 includes a field 410 which informs the user that he is not currently subscribed to the selected program. That is, the user must order the program. A field 420 informs the user that he has different options in ordering the program. Fields 430-460 present the options. A field 440 presents a first option wherein the movie may be purchased as an impulse pay-per-view (IPPV) program with the cost being deducted from an available cash credit balance. The user is thus informed of the cash cost of the movie and the available cash credit balance. The program can be purchased as long as there is a sufficient cash credit balance.

A field 450 presents a second option, where the program may be purchased using digital coupons alone. The user is informed of the coupon cost of the movie and the available coupon credit balance. The program can be purchased as long as there is a sufficient coupon credit balance. The digital coupons are referred to here as "TV" coupons.

A field 460 presents a third option, where the program may be purchased using a combination of cash and digital coupons. The user is informed of the cost of the movie using both coupons and cash, and the available cash credit balance and coupon credit balance. While only one cash/coupon combination is provided in field 460, it will be understood that other combinations may also be provided. In fact, the coupons may be assigned a cash value for this purpose.

In another option, not shown, a subscriber may order a PPV program for a discount if the subscriber is willing to have commercial messages appear which would not otherwise be present. For example, a commercial message using teletext may appear on the bottom portion of the screen when viewing a PPV movie. Or, with VOD, the PPV movie chosen may have periodic commercial message breaks when the discounted program is selected, whereas no commercials would be provided otherwise.

FIG. 5 is another on-screen display for a user interface in accordance with the present invention. Here, the display 500 provides information on the number of coupon credits which have been accumulated while viewing different channels. For example, the various program service providers may

provide viewers with coupons based on the number of hours of that service provider which is viewed per week, and/or which programs were viewed.

Fields 510 and 530 list the various program service providers, while fields 520 and 540 list the number of coupon credits which have been accumulated. For example, for the service provider Home Box Office (HBO), there is a balance of four coupons. In this manner, the program service providers may compete to encourage viewership. For example, when launching a new program, additional coupons may be provided. Furthermore, coupons may be accumulated based on the time of day or day of week that programs are viewed. Moreover, program service providers that are commonly owned may award coupons to encourage viewership of their programs.

FIG. 6 is yet another on-screen display for a user interface in accordance with the present invention. The display 600 provides an example of the variety of items from which the subscriber may select using the digital coupons of the present invention. Moreover, each of the program service providers along with other interested parties may offer their own items. A field 610 indicates that the particular display 600 is that of the service provider Cable News Network (CNN). A field 620 indicates the current coupon credit balance, while a field 630 indicates the items that may be obtained, and field 640 indicates the number of coupons needed to obtain each item.

Thus, the user may redeem the digital coupons for a wide variety of items, including additional programming that can be communicated to, or accessed by, the terminal as well as non-programming items which can be delivered to the user's home, e.g., by mail.

Some items may not require any digital coupons. For example, a field 650 describes product information which can be communicated to the subscriber's terminal or delivered to the subscriber's home at no cost. However, when the subscriber requests the product information, the usage pattern data is updated and may be subsequently provided to the usage pattern data accounting function 125 of FIG. 1, where it may be used for marketing purposes.

FIG. 7 is a flowchart illustrating a method for providing digital coupons in accordance with the present invention. The flowchart describes an embodiment where an initial cash credit balance is provided to a terminal, for example, on a monthly basis. Then, when the user desires to view programming such as PPV programming that has an associated cost, the cost is deducted from the cash credit balance. Furthermore, when the user meets the preconditions of the digital coupon information as determined by the usage pattern data, a coupon credit balance is accumulated. The coupon credit balance may be used to purchase additional program services in lieu of cash, or, optionally, to defray the cost of programs already purchased. In the latter case, the coupon credits may be assigned a cash value.

At block 705, the controller at the transmitter delivers an initial cash credit balance to the terminals. The amount delivered to each terminal may be different and may be based, for example, on past purchasing habits. At block 710, the controller delivers the digital coupon information to the terminals. Again, different terminals may receive different coupon data according to demographic factors and the like. At block 720, the terminal usage pattern is monitored and recorded. In particular, events which meet the preconditions of the digital coupons are recorded, while other data indicative of user habits may also be recorded.

The digital coupon preconditions may account for a variety of events, such as whether the subscriber has pur-

chased a given number N of PPV programs in the last M days (block 722), in which case a digital coupon credit "1" is awarded at block 724. It will be appreciated that different types and amounts of coupons may be awarded according to the particular precondition which the viewer meets. For example, some coupon credits may be more valuable than others, or may be redeemed for different benefits.

At block 726, if it is determined that the subscriber has purchased X\$ of PPV programs in the last Y days, a digital coupon credit "2" is awarded at block 728. At block 730, if the subscriber has viewed an "infomercial" for a number Z minutes, a digital coupon "3" is awarded at block 732. An "infomercial" is a commercial message that has the length and format of a regular program, e.g., such as one-half hour or more, and generally garners a relatively small audience. For marketing purposes, it is desirable to reward viewers for viewing infomercials even though there is no charge incurred for viewing the program. Optionally, coupon credit may be awarded only for the first viewing of the program, so additional coupon credits are not awarded for repetitive viewing of the same program.

At block 734, if the subscriber has upgraded from a basic programming tier to a premium programming tier, or to a higher premium programming tier, a digital coupon "4" is awarded at block 736. At block 738, if a promotional period is in progress, a digital coupon "5" is awarded at block 740. Such a promotional period would generally apply to all subscribers.

At block 750, the total amount of coupon credits is determined. At block 760, if the coupon credit balance is above zero, then at block 770, the user is prompted by the user interface (e.g., every time the television is turned on) to select among the various options which are available in redeeming the digital coupons. For example, the subscriber may order PPV programming for a discount or no charge, access premium programming for a predetermined period of time, or simply pass and take advantage of the available options at another time. The various options have been discussed above in greater detail in connection with FIGS. 4-6. In addition to the periodic prompts described above, a user will also have the capability of accessing the coupon redemption menu at any time via the remote control.

At block 780, the digital coupon balance is adjusted by the number of coupons redeemed at block 770, and the monitoring of the terminal usage pattern continues at block 720.

Note that it is possible to verify that the user is actually viewing a particular program by requiring some sort of subscriber involvement. For example, to verify that a subscriber has watched an infomercial for Z minutes, the terminal may require the subscriber to input a command to the user interface. The user interface may provide a message such as "Do you wish to continue", to which the subscriber must respond to meet the digital coupon preconditions. An internal timer within the terminal may be halted until a response is received.

For subscribers who view infomercials and the like, to ensure that only one set of coupons are awarded per program, the COUPON_RECORD_DURATION field as discussed below in Table 3 is provided to indicate a duration in which the program record of the infomercial is stored in the terminal. This precludes the same subscriber from getting repeated coupons for the same infomercial that is run again and again, while still enabling the same program ID for the infomercial to be used repeatedly.

The data delivery syntax set forth below in Tables 1-4 may be used in accordance with the present invention.

13

Tables 1-3, respectively, describe data fields which may be used when digital coupons are delivered to terminals using an EMM, an IPPV ECM purchase linkage, and a program re-key ECM. Table 4 describes data fields which may be used with all delivery methods. It should be appreciated that the syntax shown is for illustration only and that other data delivery schemes may be substituted.

TABLE 1

Syntax	Size	Description
COUPON_PROVIDER_ID	3 bytes	Identifies coupon sponsor
NEW_COUPON_CREDIT	3 bytes	Absolute number of coupons for service provider in a month
NEW_COUPON_DEBIT	3 bytes	Absolute debit for service provider in a month
COUPON_CREDIT	3 bytes	Total accrued coupons
COUPON_SEQ_NUMBER	1 byte	Epoch (time period) of coupon delivery

TABLE 2

Syntax	Size	Description
COUPON_PROVIDER_ID	3 bytes	Identifies coupon sponsor
COUPON_CREDIT	1 byte	Coupon credit remaining

TABLE 3

Syntax	Size	Description
COUPON_ID	2 bytes	COUPON_ID + COUPON_PROVIDER_ID = unique coupon ID)
COUPON_PAYOUT_DURATION	2 bytes	Time period subscriber must view program to obtain coupon credit
COUPON_RECORD_DURATION	3 bytes	Time period coupon is retained at terminal
COUPON_PROVIDER_ID	3 bytes	Identifies coupon sponsor

TABLE 4

Syntax	Size	Description
COUPON_DEBIT	2 bytes	Number of accrued coupon debits
COUPON_PACKAGE_ID	2 bytes	Type of coupon for package program
IPPV_CREDIT	2 bytes	Cash credit balance for pay-per-view
PACKAGE_PROVIDER_ID	2 bytes	Identifies service provider of package of programs
PKG_COST	1 byte	Cash charge for package program
PKG_ID	1 byte	Identifies package
PROGRAM_PAYOUT_DURATION	1 byte	Minimum time subscriber must view program to gain credit
PROGRAM_INFORMATION	2 bytes	Video/audio data of program
SHOW_COUNT	2 bytes	Count of shows purchased
VH_LIMIT	2 bytes	View History Limit before report back is mandatory
VIDEO_PROVIDER_ID	2 bytes	Identifies service provider

To thwart piracy, digital coupons may only be offered to subscribers with established impulse PPV accounts where there is a report-back capability. This can be effected, for example, by using a bit as a flag in either the group re-key EMM or Program re-key ECM.

14

The report-back feature discussed above in connection with the usage pattern data accounting function 125 of FIG. 1 allows the program service providers and network controller to monitor the audience size for different programs. The use of digital coupons can therefore allow the service providers to detect viewership patterns over a wide cross-section of programs, and not just premium shows. In other words, shows which are not available through PPV might be made available through coupons.

In the following program delivery scenarios, it is assumed that a real channel (i.e., program) must exist which can be purchased with coupons. This can be enforced by hashing the program information to generate a program key as explained further below. Therefore, a program cannot be viewed using digital coupons unless it is actually offered to coupon holders.

However, pirates may attempt to tamper with the delivery of the coupons. The main objective of the pirate is to defeat the system by providing false messages (e.g., "spoofing") to obtain digital coupons without having to perform any of the coupon preconditions. In accordance with the present invention, different ways to securely deliver the COUPON_CREDIT field to terminals are discussed.

There are three ways to deliver the digital coupons, i.e., using a group re-key EMM, an IPPV purchase linkage, or a program re-key ECM. The group re-key message technique can handle a distribution of coupons to a general population of terminals as well as providing a method that is linked to IPPV purchases. IPPV purchase linkage could be done independently from group re-key message delivery, however. The delivery of coupons via the group re-key message may be mutually exclusive from the program re-key technique since, with the program re-key technique, the network controller or PPV order processing center does not know how many coupons a subscriber might earn using the method where the coupons are generated internally by the terminal. Thus, management of group re-key based coupons cannot be handled as securely inside a terminal unless group re-key based coupons are tracked separately from program re-key based coupons.

Direct delivery of coupons through a group re-key entitlement management message (EMM) is the most straightforward way to control the delivery of coupons to subscribers. This approach is suitable for IPPV service providers who decide to reward particular subscribers based, for example, on previous purchasing volume. The service provider thus knows which particular subscribers are to receive the digital coupons and can therefore direct a unit specific EMM to each of the subscribers.

Additionally, the group re-key EMM approach is suitable for providing subscribers with digital coupons along with a designator which allows text message commercials. These on-screen displays convey advertising and can be overlaid on top of the video and audio displayed. As discussed previously, these subscribers are willing to view such commercials to obtain digital coupon benefits such as discounts on other programs. Again, the service providers know exactly which subscribers agreed to have text message commercials delivered to them, and can therefore provide them with the corresponding digital coupons through an EMM.

Moreover, using the COUPON_CREDIT and VH_LIMIT data fields, individual service providers can send digital coupons to individual subscribers. Each service provider is identified by the field VIDEO_PROVIDER_ID. If a pirate were to synthesize a group key message with a

15

false VIDEO_PROVIDER_ID and COUPON_CREDIT, thereby resulting in a bad group key, the pirate might be able to create false VIDEO_PROVIDER_ID, COUPON_CREDIT pairs inside the terminal.

One solution to the above problem is implemented using EMM authentication. In particular, if the group re-key EMM used by a transmitting satellite, for example, is hashed. The hash is then encrypted to create a signature. A pirate cannot produce a counterfeit group re-key EMM without knowledge of a terminal's unit keys, and the key hierarchy. In this case, the counterfeit message will be rejected without processing. Another way to authenticate a message is to use public key cryptography to sign or encrypt the entire message. This can also prevent the generation of counterfeit messages.

Furthermore, a pirate may use "replay" attacks using legitimately built messages. In this case, a legitimate message is saved and provided to a terminal months after the message was originally created and first used to make new COUPON_CREDIT inside the terminal. To protect against this, group sequence numbers may be incremented.

Moreover, the pirate may attempt to replay the message in the same month that it was generated. To protect against this, new COUPON_CREDIT could be tracked during a particular month. At the end of the month, it can be added to COUPON_CREDIT that was earned in previous months. When the COUPON_CREDIT FIELD is sent to the terminal during the month in the group re-key EMM, it would be the absolute coupon credit issued to a particular terminal. Moreover, an additional field, COUPON_DEBIT, may be created inside the terminal to manage the coupons from a particular service provider for that month. Another way to secure against replay attacks within the same month would be to sequence the EMMs themselves. The decoder may then be able to differentiate between a new message and one that it has seen before. Another method would be to include a date/time parameter in the EMM. As with a sequence number, this field can only go forward or stay the same, but cannot be changed to a past value.

For each individual service provider, any new COUPON_CREDIT value must be authenticated, e.g., in the group re-key message just as with the COUPON_CREDIT and VH_LIMIT fields since merely signing the message or using public key cryptography will not prevent such replay attacks. Moreover, each new coupon record should track the sequence number which indicates when it was generated. When the group key epoch occurs, the group re-key EMM that was originally used to create the coupon record will not be able to create additional coupons since the message will be old. At that time, the new COUPON_CREDIT can be added to old COUPON_CREDIT. If, during the next month, no new coupons are sent to the terminal, and all of the existing coupons are used, then the entire coupon record can be erased.

In a second digital coupon delivery method, coupons are delivered through an IPPV buy linkage. With each IPPV purchase, a bit in the program re-key message allows a service provider to deliver one or more coupons automatically and instantly to subscribers without waiting to get a report back or performing a "trip" (e.g., delivery) with coupons as in the group re-key method discussed above. If a subscriber did not have any coupons from a particular service provider before, a new service provider coupon record is made. The coupon creation process is therefore tightly linked to actual purchases of IPPV programs. After a number of coupons have been accrued, the subscriber can

16

redeem them. Typically, a service provider will offer digital coupons which can be redeemed only for that service provider's programs. However, groups of service providers may collaborate to provide interchangeable coupons if desired.

In another possible pirate attack, a pirate may attempt to manipulate the number of coupons which are awarded when performing the digital coupon preconditions, e.g., such as purchasing a number of IPPV programs. One possible solution uses a DES hash with encryption (e.g., signature) or public key encryption of the program re-key message. If the number of coupons is authenticated in the IPPV report-back, then the pirate's manipulation of this field would cause a bad cryptographic field.

If the pirate does know the group key, counterfeiting could occur but may be detectable if the view history information (e.g., usage pattern data) is used to hash the coupon value and is sent along in the report-back.

Moreover, if public key cryptography was used in the delivery of the program re-key message, then, even if the pirate knew the group public key, a message still could not be synthesized since the group private key would not be known. Public key cryptography has a distinct advantage over secret key cryptography since the group encrypt or private key is not in the terminal. Consequently, VLSI probing and other attacks against the terminal cannot reveal the key.

In a third delivery method in accordance with the present invention, digital coupons are delivered in conjunction with extended commercial programs known as "infomercials." Preferably, a subscriber is rewarded with digital coupon credits only after viewing the program for a specific amount of time. Furthermore, to prevent the subscriber from simply tuning in the program and walking away, it might be advantageous to require some sort of subscriber involvement such as a control input which is requested by the user interface.

A pirate may be able to alter code in a non-secure processor to automatically provide the subscriber involvement control signal. However, the amount of time that the program must be viewed, or at least tuned in, can be secured. To do this, there is no need to track the maximum time that the program lasts since the infomercial service provider is essentially paying the subscriber to view the program. The PROGRAM_PAYOUT_DURATION field can be loaded into a countdown timer to enforce the minimum viewing time requirement of the digital coupon preconditions. The coupons are thus issued when the timer counts down to zero, and the timer counts down only when the infomercial channel is tuned in. Essentially, this ties up the terminal to tune in the infomercial and precludes it from tuning in another channel.

Furthermore, the COUPON_RECORD_DURATION field is required to determine when the program record should be expunged from the secure processor's memory.

A pirate may attempt to manipulate the field in the program re-key ECM, which indicates how many coupons are to be awarded when viewing the infomercial. One possible solution is to use a DES hash (e.g., signature) or public key encryption of the program re-key message. Like the other attacks described above, signing the program re-key message makes it hard for the pirate to counterfeit the program re-key message without knowledge of the group secret key or private key. Moreover, if public key cryptography is used in the delivery of the program re-key message, then, even if the group public key was known by a pirate, a

message could not be synthesized since the group private key is not known.

In another possible pirate attack, the pirate records legitimate program messages, and repeatedly plays back the messages to the terminal. The pirate may modify the terminal to provide control inputs directly to the chip or via the user interface to increase the number of coupons held by the chip. One solution to this attack is to create and store a program record in memory. In particular, the COUPON_CREDIT field is used to authenticate the number of coupons being awarded. In addition to COUPON_PKG_ID and COUPON_PROVIDER_ID, two duration timers are needed instead of one. One timer, COUPON_PAYOUT_DURATION, tracks how long the subscriber must be tuned to the program before coupons are awarded, and the other time, COUPON_RECORD_DURATION, tracks when the program record can be expired from memory. The amount of time that a record should be retained might be two months, for example.

Delivery of program re-key messages by public key is a safer mechanism. A pirate would need to cryptographically search for the group private key to alter program re-key messages. The group private key is not delivered to any terminal anywhere in the network. The length of the group public keys delivered could expand according to the perceived piracy threat. And, the group public and private keys may be changed through the delivery of new EMMs. If there is a system breach, the infomercial feature could be abandoned simply by making program re-key ECMs with the coupon issuing feature missing, or not allowing IPPV purchases with coupons.

In the above discussion, it was seen that there are three distinct methods for delivering coupons to the terminals. The first is group re-key EMM based, the second is tightly tied to IPPV authentication, and the third is Program Re-key ECM based using the "infomercial" concept.

The group re-key method is similar to how IPPV is implemented with the only absolute COUPON_CREDIT given, and requiring a COUPON_DEBIT field to exist inside the terminal for each service provider with a COUPON_PROVIDER_ID.

The IPPV purchase linkage method is a hybrid between the group re-key method and the program re-key method since it takes advantage of IPPV authentication that is already done and securely authenticated inside the terminal, and yet is delivered by a program re-key ECM with the appropriate parameters set. Coupons using this method can only be delivered through a real IPPV purchase.

With the program re-key method, coupon redemption may or may not be tied to the view history report-back. For auditing of viewership, coupon redemption is tied to the report-back since a communication link such as a telephone network is required.

Accordingly, it can be seen that the present invention provides a system for transmitting digital coupons to subscriber terminals for various promotional purposes. By delivering and managing the coupons electronically, the coupons are more likely to be used by the subscribers, and distribution and handling costs for the promoters are significantly reduced. Subscriber loyalty can be rewarded, while subscribers can also be selectively targeted to try out programming in which they are likely to have a special interest. Subscribers can be even be encouraged to view commercial programming such as infomercials. Additionally, with an optional report back feature, terminal usage pattern data can be retrieved and analyzed to deter-

mine the effectiveness of the promotions and to gather additional demographic and individual data. Furthermore, the integrity of the scheme can be assured with various encryption techniques.

Although the invention has been described in connection with various specific embodiments, those skilled in the art will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

For example, accounting of the coupon credit balance may be maintained by the network controller or other entity apart from the terminal. This accounting may be updated real-time as the coupon balance changes, or periodically, such as where an automatic telephone report back capability is provided.

What is claimed is:

1. A transmitting end apparatus of a subscriber television network, comprising:

a programming services data function for providing programming services;

a digital coupon information function for providing digital coupon information; and

a controller; wherein:

said controller is responsive to said programming services function for transmitting the programming services to a plurality of subscriber terminals of the network via a communication channel;

said programming services are adapted to be recovered by said subscriber terminals;

said controller is responsive to said digital coupon information function for delivering the digital coupon information to said terminals via said communication channel;

said digital coupon information defines preconditions for enabling said terminals to obtain credits when recovering the programming services; and

said digital coupon information enables the terminals to maintain a running credit balance according to credits obtained and credits redeemed.

2. The apparatus of claim 1, wherein:

the credits are redeemable by users at the respective terminals for obtaining programming services at a reduced charge.

3. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals recover particular programming services to obtain credits.

4. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals recover a specified number of the programming services to obtain credits.

5. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals recover the programming services for a specified duration to obtain credits.

6. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals incur a specified amount of charges in recovering the programming services to obtain credits.

7. The apparatus of claim 1, further comprising:

encryption means operatively associated with said controller for encrypting said digital coupon information and said programming services, prior to transmission to the terminals, according to a common cryptographic key.

19

8. The apparatus of claim 1, wherein:
said digital coupon information function provides different digital coupon information for different ones of the terminals.
9. The apparatus of claim 8, further comprising:
a usage pattern accounting center operatively associated with said controller, and adapted to receive usage pattern data from the terminals; wherein:
said digital coupon information function is responsive to said usage pattern accounting center and said usage pattern data for providing the different digital coupon information.
10. The apparatus of claim 9, wherein:
the usage pattern data indicates a viewing history of the programming services at the terminals over a specified time period.
11. The apparatus of claim 1, wherein:
the controller transmits data to the terminals via the communication channel for establishing an initial credit balance at the terminals.
12. A transmitting end method for a subscriber television network, comprising the steps of:
providing programming services and digital coupon information at the transmitting end; and
transmitting the programming services and the digital coupon information from the transmitting end to a plurality of subscriber terminals of the network via a communication channel; wherein:
the programming services are adapted to be recovered by the subscriber terminals;
the digital coupon information defines preconditions for enabling the terminals to obtain credits when recovering the programming services; and
the digital coupon information enables the terminals to maintain a running credit balance according to credits obtained and credits redeemed.
13. The method of claim 12, wherein:
said credits are redeemable by users at the respective terminals for obtaining programming services at a reduced charge.
14. The method of claim 12, wherein:
the preconditions require that the respective terminals recover particular programming services to obtain credits.
15. The method of claim 12, wherein:
the preconditions require that the respective terminals recover a specified number of the programming services to obtain credits.
16. The method of claim 12, wherein:
the preconditions require that the respective terminals recover the programming services for a specified duration to obtain credits.
17. The method of claim 12, wherein:
the preconditions require that the respective terminals incur a specified amount of charges in recovering the programming services to obtain credits.
18. The method of claim 12, comprising the further step of:
encrypting said digital coupon information and said programming services at the transmitting end, prior to transmission to the terminals, according to a common cryptographic key.
19. The method of claim 12, comprising the further step of:
providing different digital coupon information for different ones of the terminals.

20

20. The method of claim 19, comprising the further step of:
receiving usage pattern data from the terminals at the transmitting end; wherein:
the different digital coupon information is provided in response to the usage pattern data.
21. The method of claim 20, wherein:
the usage pattern data indicates a viewing history of the programming services at the terminals over a specified time period.
22. The method of claim 12, comprising the further step of:
transmitting data from the transmitting end to the terminals via the communication channel for establishing an initial credit balance at the terminals.
23. A subscriber terminal in a subscriber television network, comprising:
means for recovering programming services and digital coupon information from a transmitting end of the network via a communication channel;
means for processing said digital coupon information to determine preconditions thereof for enabling the terminal to obtain credits when recovering the programming services; and
means for maintaining a running credit balance according to credits obtained and credits redeemed.
24. The terminal of claim 23, wherein:
said credits are redeemable by a user at the terminal for obtaining programming services at a reduced charge.
25. The terminal of claim 23, wherein:
the preconditions require that the terminal recover particular programming services to obtain credits.
26. The terminal of claim 23, wherein:
the preconditions require that the terminal recover a specified number of the programming services to obtain credits.
27. The terminal of claim 23, wherein:
the preconditions require that the terminal recover the programming services for a specified duration to obtain credits.
28. The terminal of claim 23, wherein:
the preconditions require that the terminal incur a specified amount of charges in recovering the programming services to obtain credits.
29. The terminal of claim 23, wherein:
the digital coupon information is customized for the terminal.
30. The terminal of claim 23, further comprising:
monitoring means for monitoring a usage pattern of the terminal to determine if said preconditions have been satisfied; wherein:
said maintaining means is responsive to said monitoring means for maintaining said running credit balance.
31. The terminal of claim 30, further comprising:
a communication interface for communicating data indicative of said usage pattern from said monitoring means to a usage pattern accounting center at the transmitting end; wherein:
said usage pattern data enables the transmitting end to customize the digital coupon information provided to the terminal.
32. The terminal of claim 30, wherein:
the usage pattern indicates a viewing history of the programming services at the terminal over a specified time period.

21

33. The terminal of claim 23, wherein:
said maintaining means is adapted to establish an initial credit balance in response to data received from the transmitting end.
34. The terminal of claim 23, further comprising:
a user interface for enabling the terminal to redeem said credits according to a user input.
35. The terminal of claim 23, wherein said digital coupon information and said programming services are encrypted at the transmitting end according to a common cryptographic key, further comprising:
decryption means for decrypting said digital coupon information and said programming services.
36. The terminal of claim 35, further comprising:
authentication means for cryptographically authenticating said digital coupon information.
37. The terminal of claim 36, wherein:
said authentication means authenticates said digital coupon information according to a group key.
38. The terminal of claim 36, wherein:
said authentication means authenticates said digital coupon information according to a public key.
39. The terminal of claim 23, wherein:
said programming services include programs which are encrypted according to associated program re-keys; and
at least a particular one of said program re-keys is transmitted to the terminal from the transmitting end to allow the terminal to decrypt and recover the associated program using said program re-key; and
said digital coupon information is transmitted to the terminal with said program re-keys.
40. A data processing method for a terminal in a subscriber television network, comprising the steps of:
recovering programming services and digital coupon information from a transmitting end of the network via a communication channel;
processing said digital coupon information to determine preconditions thereof for enabling the terminal to obtain credits when recovering the programming services; and
maintaining a running credit balance according to credits obtained and credits redeemed.
41. The method of claim 40, wherein:
said credits are redeemable by a user at the terminal for obtaining programming services at a reduced charge.

22

42. The method of claim 40, wherein:
the preconditions require that the terminal recover particular programming services to obtain credits.
43. The method of claim 40, wherein:
the preconditions require that the terminal recover a specified number of the programming services to obtain credits.
44. The method of claim 40, wherein:
the preconditions require that the terminal recover the programming services for a specified duration to obtain credits.
45. The method of claim 40, wherein:
the preconditions require that the terminal incur a specified amount of charges in recovering the programming services to obtain credits.
46. The method of claim 40, wherein:
the digital coupon information is customized for the terminal.
47. The method of claim 40, comprising the further step of:
monitoring a usage pattern of the terminal to determine if said preconditions have been satisfied; wherein:
said maintaining step is responsive to said monitoring step.
48. The method of claim 47, comprising the further step of:
communicating data indicative of said usage pattern from the terminal to a usage pattern accounting center at the transmitting end; wherein:
said usage pattern data enables the transmitting end to customize the digital coupon information provided to the terminal.
49. The method of claim 47, wherein:
the usage pattern indicates a viewing history of the programming services at the terminal over a specified time period.
50. The method of claim 40, comprising the further step of:
establishing an initial credit balance in response to data received from the transmitting end.
51. The method of claim 40, comprising the further step of:
receiving a user input to redeem the credits.

* * * * *



US006057872A

United States Patent [19]
Candelore

[11] **Patent Number:** **6,057,872**
 [45] **Date of Patent:** **May 2, 2000**

[54] **DIGITAL COUPONS FOR PAY TELEVISIONS**

0 833 511 4/1998 European Pat. Off. .
 WO 96/32702 10/1996 WIPO .

[75] **Inventor:** **Brant Candelore, San Diego, Calif.**

[73] **Assignee:** **General Instrument Corporation,**
Horsham, Pa.

Primary Examiner—Nathan Flynn
Attorney, Agent, or Firm—Barry R. Lipsitz; Ralph F. Hoppin

[21] **Appl. No.:** **08/890,066**

[22] **Filed:** **Jul. 9, 1997**

[51] **Int. Cl.⁷** **H04N 7/10**

[52] **U.S. Cl.** **348/3; 348/10**

[58] **Field of Search** 709/217–219;
 345/327, 328; 348/6, 7, 8, 3, 1, 10, 12,
 13, 2; 455/4.1, 4.2, 5.1, 52; H04N 7/10

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,876,592 10/1989 Von Kohorn .
 5,128,752 7/1992 Von Kohorn .
 5,249,044 9/1993 Von Kohorn .
 5,260,778 11/1993 Kauffman et al. .
 5,532,735 7/1996 Blahut et al. 348/13
 5,604,542 2/1997 Dedrick .
 5,610,653 3/1997 Abecassis 348/110
 5,838,314 11/1998 Neel et al. 345/327

FOREIGN PATENT DOCUMENTS

0 656 728 6/1995 European Pat. Off. .

51 Claims, 7 Drawing Sheets

[57] ABSTRACT

Digital coupons are selectively transmitted in a communication network to subscriber terminals for promotional purposes. Subscribers automatically receive coupon credits when they meet the preconditions of the digital coupons. Free or reduced price pay-per-view (PPV) programming in particular may be provided when a subscriber purchases a given number of PPV programs at a regular price. The terminals maintain a running balance of available coupon credits and inform the subscriber via a user interface of the available balance. Subscribers can be rewarded for viewing commercial messages by awarding coupons which can be immediately redeemed for PPV programs. With an optional report back capability, terminal usage pattern data can be retrieved and analyzed by program service providers to determine the effectiveness of the promotions and to gather additional demographic and individual data. The integrity of the scheme is assured with encryption techniques.

400

410 YOU ARE NOT SUBSCRIBED TO THE PROGRAM.

420 HOW DO YOU WISH TO VIEW THE MOVIE?

430 YOUR OPTIONS ARE:

440 a)IMPULSE PAY-PER-VIEW
 -THE COST IS \$3.50 FOR THE MOVIE.
 -YOU HAVE \$27.50 CREDIT.

450 b)COUPONS
 -THE COST IS 7 TV COUPONS.
 -YOU HAVE 13 TV COUPONS.

460 a)IMPULSE PAY-PER-VIEW WITH DISCOUNT
 -THE COST IS \$1.50 WITH 4 TV COUPONS.
 -YOU HAVE \$27.50 CREDIT AND
 13 TV COUPONS.

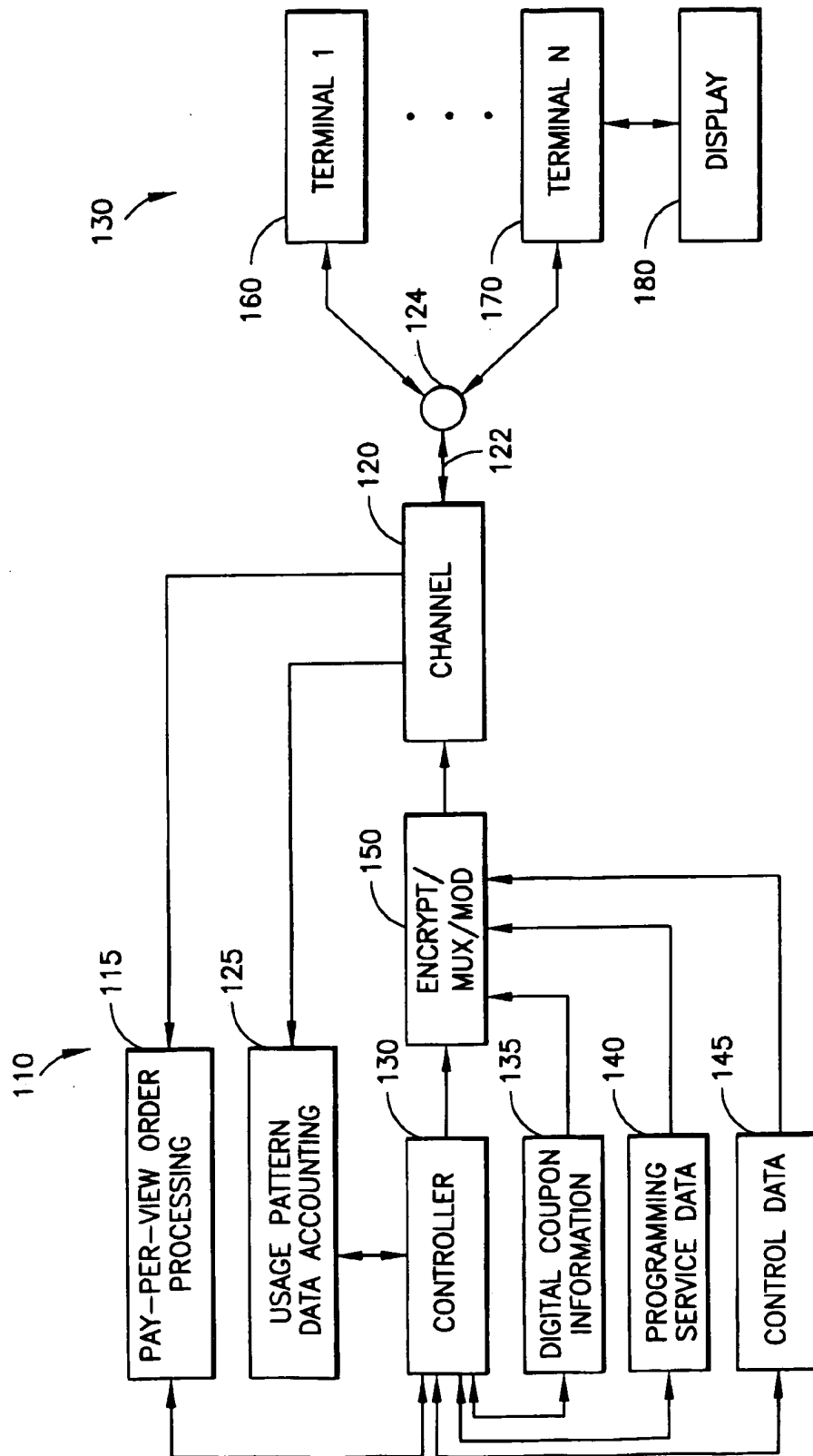
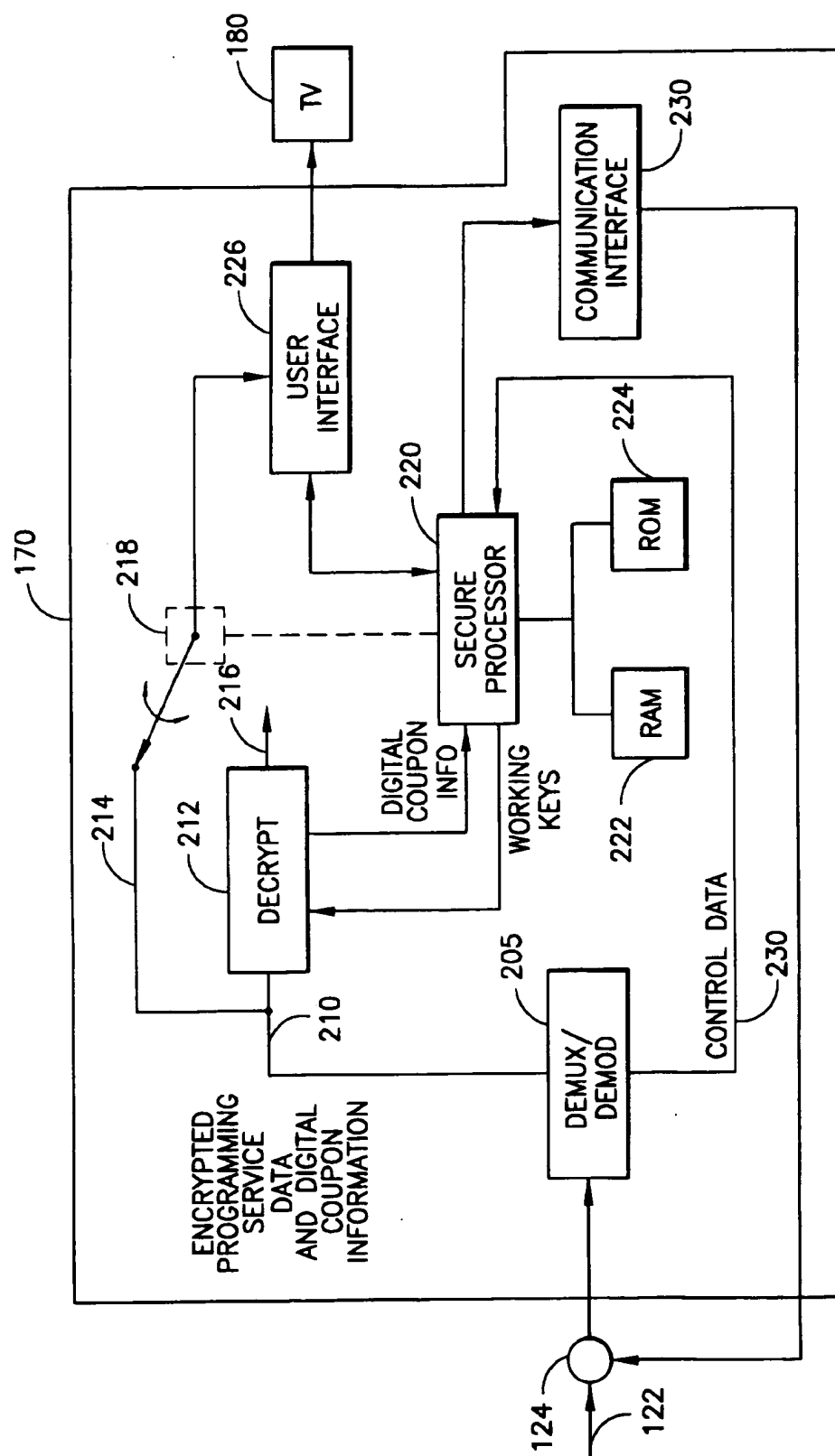


FIG. 1



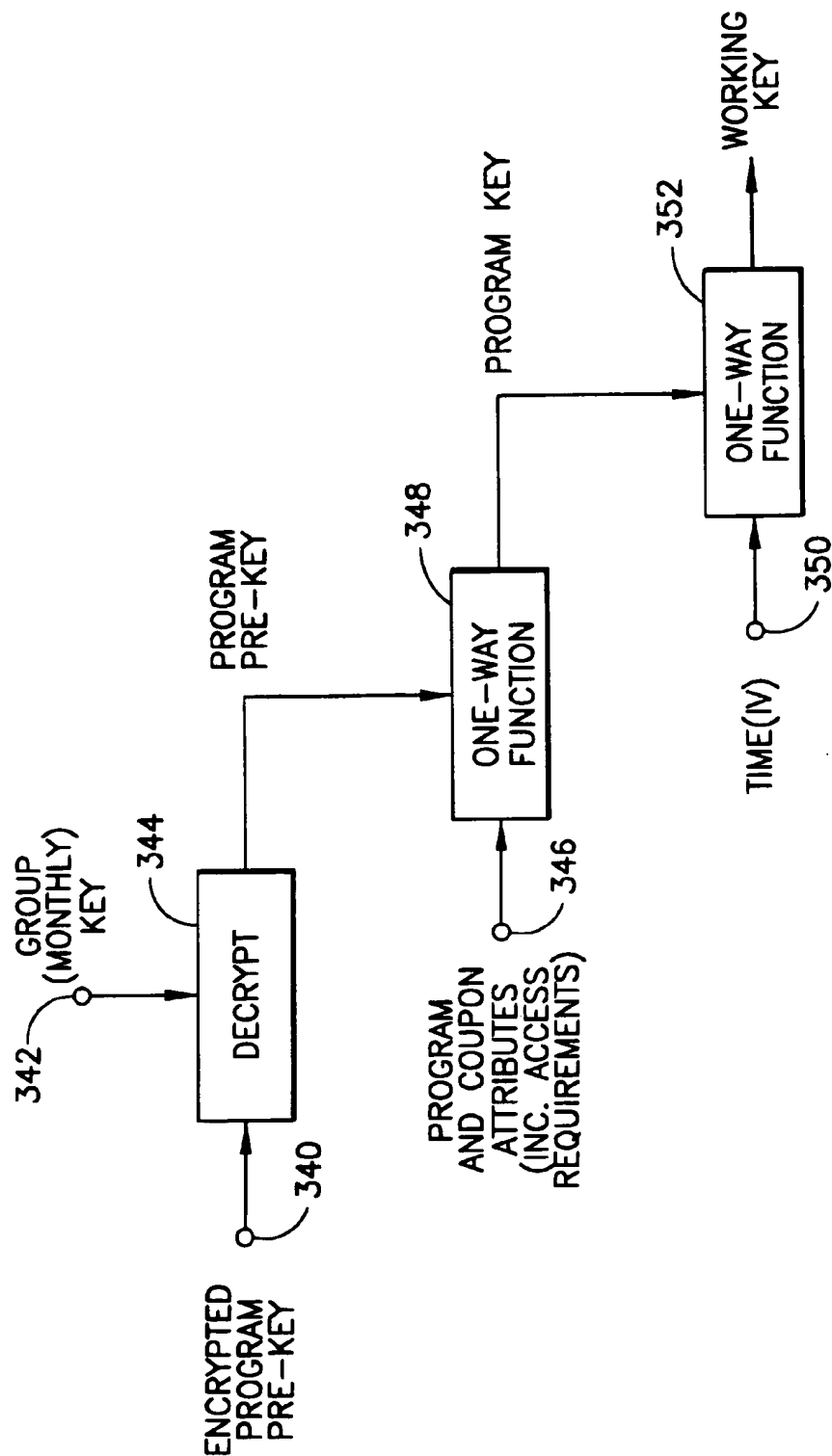


FIG. 3

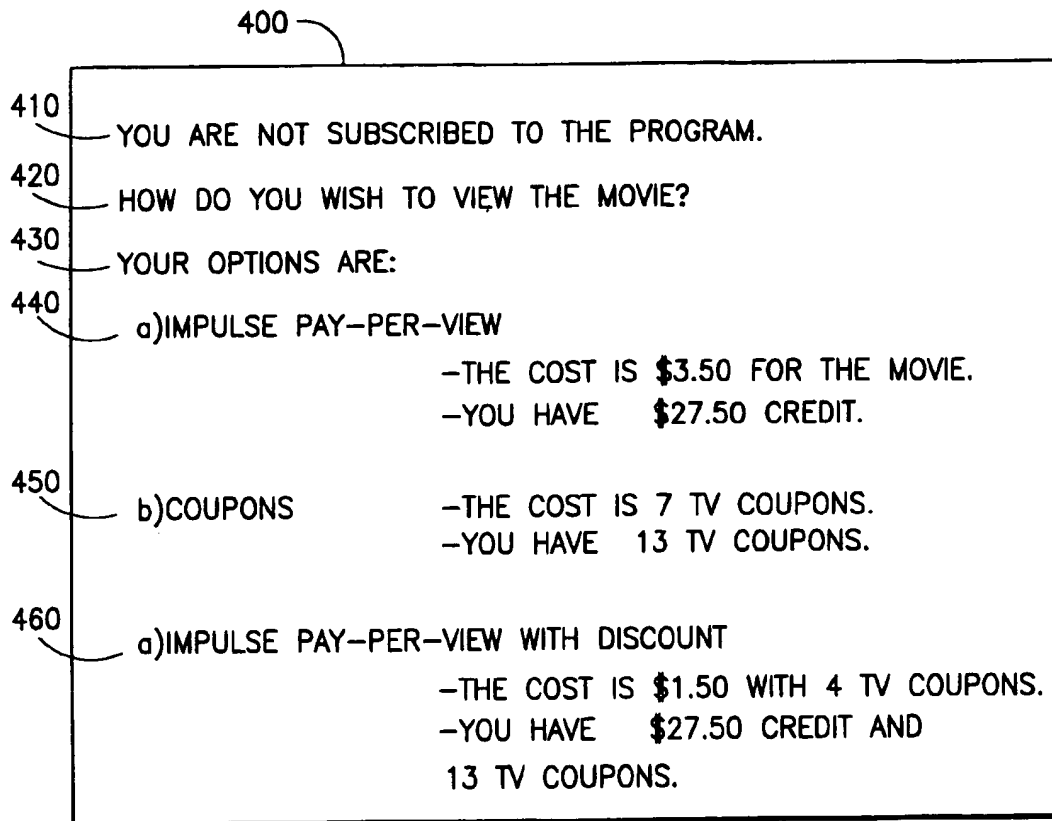


FIG.4

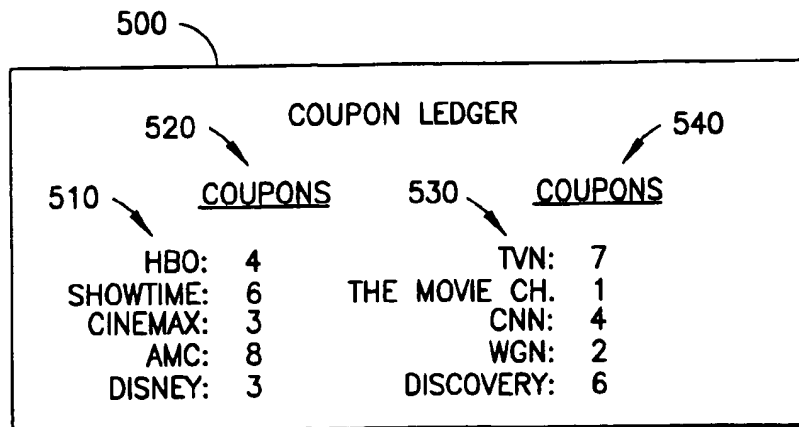


FIG.5

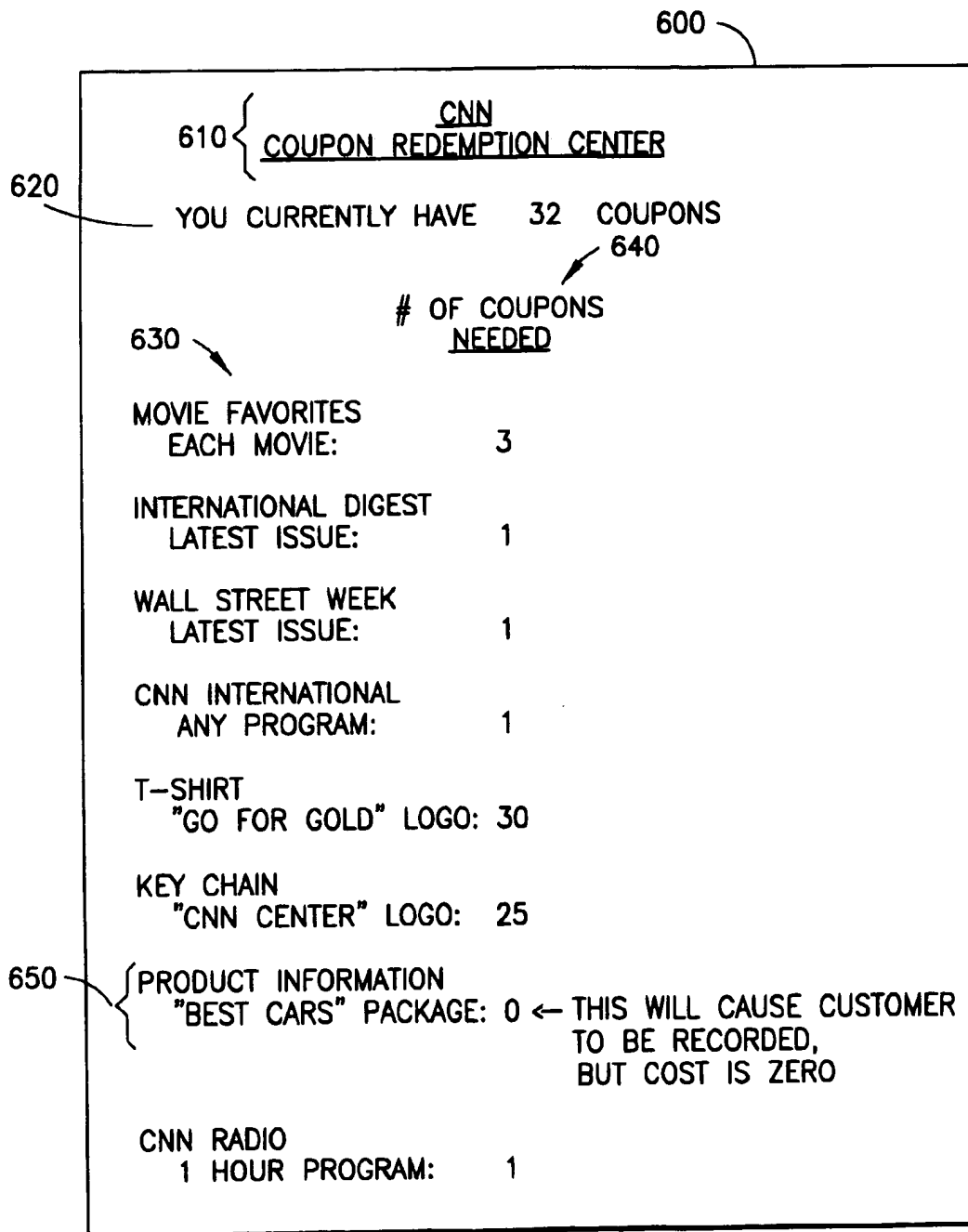
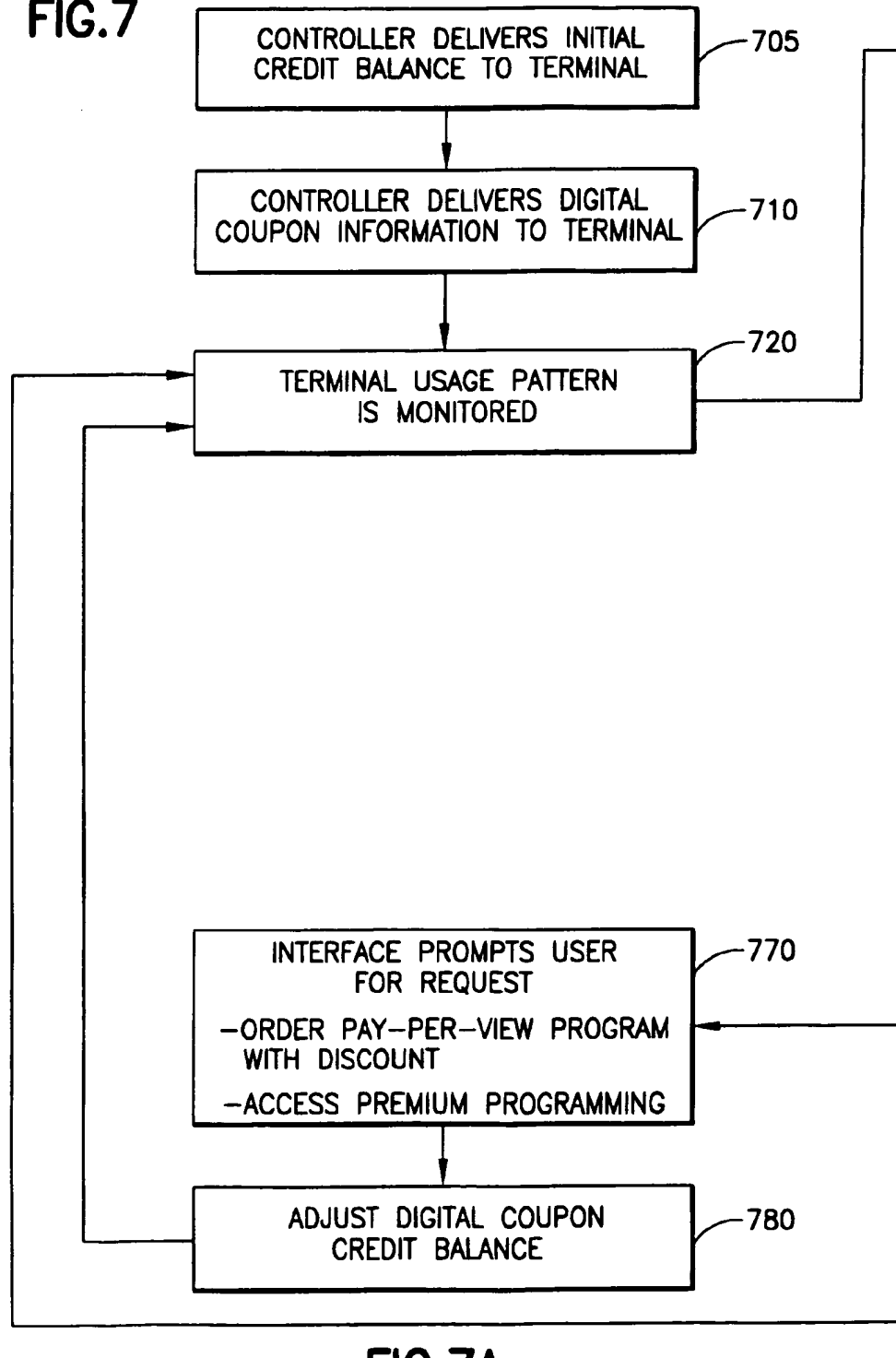


FIG. 6

FIG.7A **FIG.7B****FIG.7****FIG.7A**

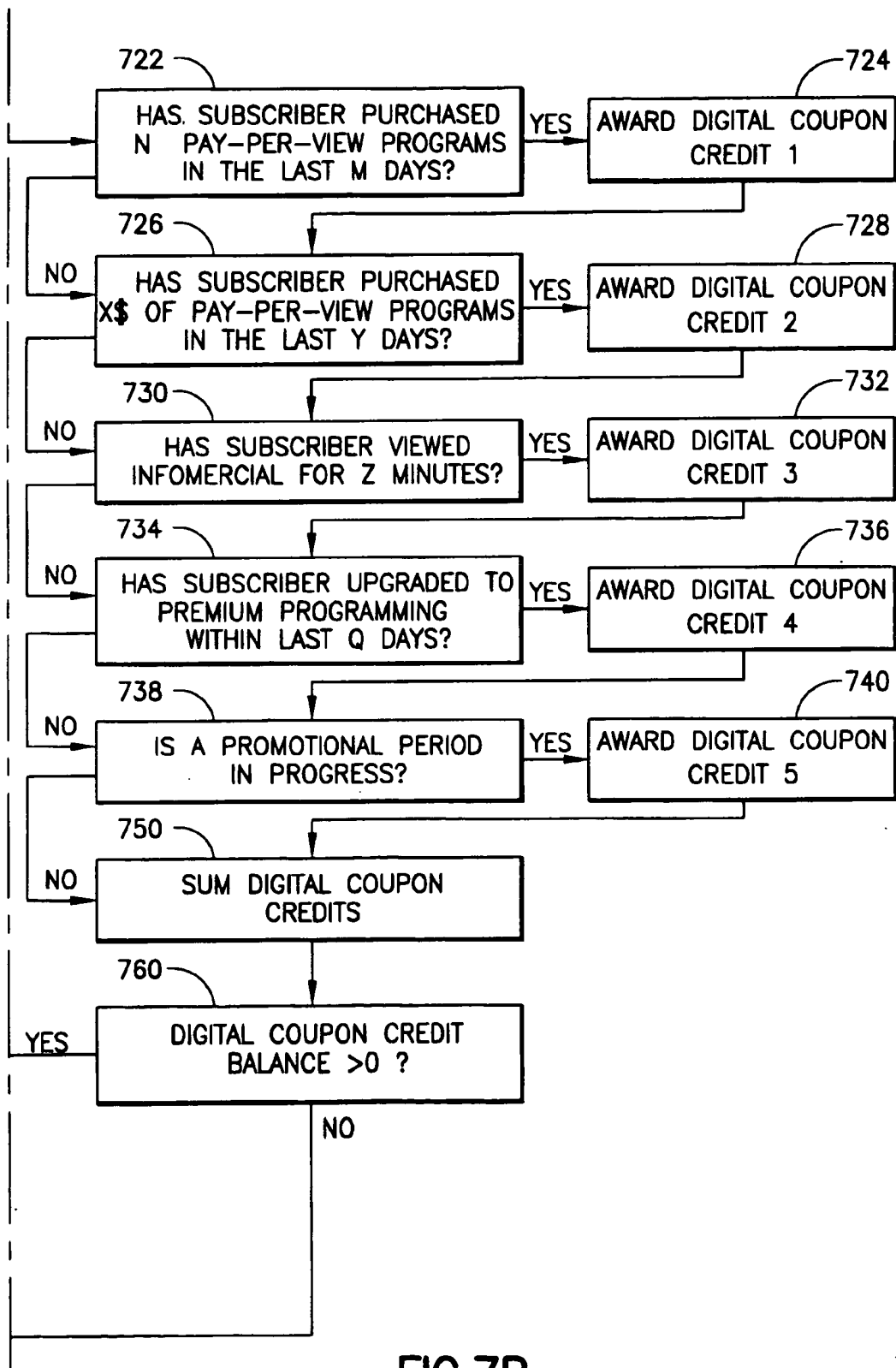


FIG. 7B

DIGITAL COUPONS FOR PAY TELEVISIONS

BACKGROUND OF THE INVENTION

The present invention relates to communications networks such as cable television, satellite television and computer networks over which services are available for a fee. In particular, an apparatus and method are presented for allowing users of services such as pay television to obtain credits when viewing particular programs. The invention enables service providers to transmit credit information in the form of "digital coupons" to individual subscriber terminals to promote particular programs and reward viewer loyalty.

Cable and satellite television networks where video services are available for a fee are well known. Also well known are computer network services such as CompuServe, Prodigy, America Online, Knight-Ridder Information Service, and others where databases, banking and shopping services can be accessed and e-mail and the like can be communicated, all for a fee. In the past, some networks have provided services on a free trial basis. For example, during promotional periods lasting for one or two days, premium programming services such as movie or sports channels could be viewed by subscribers who normally would have to pay an additional charge to receive such programming. In most cases, this is done by placing the entire service into some sort of promotional scrambling mode where the programs are either not scrambled, i.e. in-the-clear, or use fixed keys which are known to all subscriber terminals. For example, in a broadcast environment, service providers do not know which existing customer or potential new customer is attempting to access a particular service. Even if feedback could be obtained, for example, using a telephone line or some upstream path, there would be too many transactions of customers tuning in and out of services for the service provider to usefully analyze.

Consequently, the service must usually be placed in a scrambling mode which allows free accessed by everyone, including potential new customers and even existing customers, or at least a large defined group. Moreover, an extended period of free service time is usually needed to effectively promote services since the different programs which are made available during the free preview will appeal to different interest, demographic, and age groups of viewers. For example, some viewers may prefer to see action movies while others prefer to see comedies. Thus, it is necessary to provide a wide variety of free programming over an extended period of time to effectively encourage viewers to subscribe to the premium programming services for an additional monthly charge.

During the free preview period, renewal and new subscriptions rates may be reduced to further motivate the customer since the customer may otherwise wait until after the free preview period is over to order new services which may, in turn, stress the call handling capability of the service provider's subscription center.

Additionally, various programs may be offered on an individual or a-la-carte pay-per-view (PPV) basis, where the subscriber pays a fee to view a single program. The customer may either call ahead to the subscription center to have a specific authorization or entitlement for a single program sent to the customer's terminal, or the customer can arrange to have a certain amount of monetary credit downloaded into the customer's terminal. With the selection of PPV program, the pre-stored credit amount in the terminal is reduced. Such PPV may be offered at fixed times or staggered times with

so-called Near Video On Demand (NVOD). Also programs may be delivered essentially instantaneously with Video On Demand (VOD).

In VOD system systems, the program can be delivered on demand to a specific subscriber when that subscriber communicates a buy signal to a video server located at a cable television system headend. The buy signal may be communicated, for example, through an available upstream channel in a cable television network, or via a telephone line.

Various marketing techniques have been used to encourage subscribers to purchase pay-per-view programs. PPV usually are more profitable for the service provider than subscription services. These marketing techniques include providing the subscriber with a credit on his monthly statement when the subscriber purchases a predetermined number of PPV programs, or spends a predetermined amount of money on PPV programs. Or, the subscriber may be mailed a paper coupon which the subscriber can later mail back to the network billing department to obtain a discount after the subscriber has met the preconditions for redeeming the coupon. For example, the paper coupon may entitle the subscriber to a credit of one-half the price of a PPV program when one PPV program is purchased at the regular price.

While such marketing techniques can be effective, some subscribers may become accustomed to receiving paper coupons and other discounts on their monthly statements and may then resist paying higher fees when such discounts are not offered. In other words, they will only buy if they get a coupon. It would be desirable to reward the subscribers after they have met some predetermined conditions. Additionally, it is not easy to selectively target groups of subscribers or individual subscribers, without making the entire service free, or to monitor the effectiveness of such promotions. Moreover, the effectiveness of conventional promotions may be reduced because the realization of the discount by the subscriber is delayed, typically for a number of weeks due to delays in the billing cycle. Furthermore, paper coupons are difficult to organize and handle and are easily lost.

Accordingly, it would be desirable to provide a method and apparatus for allowing selective targeting of promotions of programming services to particular subscribers or groups of subscribers without placing services in free mode, or using paper coupons. The system should allow subscribers to receive an immediate credit when a predetermined viewing pattern has been met. The system should reward subscriber loyalty and encourage subscribers to purchase additional programming services such as PPV programs and/or additional levels of service, such as premium programming services.

The system should also organize the credits in a way to allow the subscriber to take a quick inventory, and should inform the subscriber when a service is available through the promotion. The system should allow flexibility as to how the credits may be used, for example, in regard to the variety of shows, times, and dates the programming may be accessed.

Furthermore, it would be desirable to provide a system for monitoring the success of such promotions, gain feedback on subscriber viewing habits, and determine the viewership (e.g., audience size) of particular programs. The system should employ cryptographic techniques to thwart unauthorized persons (e.g., pirates) who attempt to tamper with the system for illicit gain.

The present invention provides a system having the above and other advantages.

SUMMARY OF THE INVENTION

In accordance with the present invention, an apparatus and method are presented for allowing users of services such

as pay television to obtain credits when viewing particular programs. The invention enables program service providers to transmit credit information in the form of "digital coupons" to individual subscriber terminals to promote particular programs and reward viewer loyalty.

A communication system in accordance with the present invention includes a controller for transmitting program services to a plurality of subscriber terminals via a communication channel. The program service may include television programs which are broadcast or continuously transmitted on a predetermined schedule, pay-per-view programs which require specific user selection and either a local transacted or remotely transacted purchase, Near Video-On-Demand which is pay-per-view offered at staggered broadcast times, and Video-On-Demand services, which are transmitted only in response to a user request, or other electronic information such as computer software.

The communication channel may include a cable plant and/or satellite link, for example. The program services can be selectively recovered by the subscriber terminals. For example, a subscriber may select a particular program to view by tuning in the corresponding channel using an on-screen interface, e.g. Electronic Program Guide (EPG), and a remote control unit, or by transmitting a buy order for either PPV or Video-On-Demand programming.

The controller can deliver digital coupon information to the terminals along with program service data using any available technique, such as frequency or time multiplexing. The digital coupon information allows the terminals to obtain credits when recovering particular programs as defined by preconditions of the digital coupon information. For example, the subscriber may receive a credit for one free PPV program when the precondition of purchasing five PPV programs at regular prices has been met. The terminal automatically tracks the balance of coupon credits as coupons are awarded and redeemed. The credits are usable in obtaining program services at a reduced charge (e.g., at a discount or free).

Each terminal includes a processor which monitors a usage pattern (e.g., viewing history) of the terminal to determine if the preconditions of the digital coupon information have been satisfied. For example, the usage pattern may indicate which programs have been recovered by the terminal within the last month, or some other period, or the length of time that a particular program, or program service (e.g., channel) was viewed. The terminal may simply grant coupons based on the purchase of a PPV program, or based on the amount of time spent viewing an infomercial. The credits are thus awarded when there is a correlation between the usage pattern and the preconditions of the digital coupon information.

A user interface such as a graphical user interface (e.g., on-screen display) may be provided to allow the subscriber to selectively redeem the credits. For example, the user may have a variety of options from which to choose, where a cash balance and/or a coupon balance are redeemed in full or in part. The user interface can also be used to obtain a confirmation of user involvement. For example, to verify that the subscriber is still viewing a program, he may be periodically required to provide some sort of control input as the program is displayed.

When the program services include individual programs which can be individually recovered by the terminals, such as with a PPV scheme, the coupon credits are awarded when the usage pattern indicates that a terminal has recovered a particular number of such individual programs, or a particu-

lar amount of charges. This allows a coupon credit to be awarded whenever a PPV program has been accessed. One or more coupons may need to be redeemed in order to access a program.

To allow program service providers and advertisers to obtain and analyze the terminal usage data, a usage pattern accounting center which is associated with a network controller may be provided. The usage pattern accounting center can receive usage pattern data from the terminals via a communication link, such as an upstream path in the channel over which the program services are transmitted, or a telephone network. This is especially useful for determining the viewership of commercials or infomercials wherein the cost of running the ad in a program is oftentimes a function of the estimated viewing audience.

Moreover, the network controller can control the delivery of the digital coupon information to the terminals based on the received usage pattern data. In this case, the network controller can deliver the digital coupons directly to the terminal in a similar fashion as with other entitlements such as subscription entitlements, PPV entitlements, and credit information. For example, subscribers who demonstrate a preference for sports programs can receive digital coupon information which provides discounts for future special sports events.

The controller can thus deliver different digital coupon information to the different subscriber terminals based on the usage pattern data or other demographic or individual data which has been compiled by other means. The digital coupon information can provide different preconditions for obtaining the same credits, or the same preconditions for obtaining different credits. For example, it is possible to reward favored subscribers such as those who purchase relatively more programming by providing the favored subscribers with more coupons than other, less favored, subscribers when the same viewing preconditions are met.

Various cryptographic techniques may also be employed to prevent unauthorized access to the digital coupons.

A corresponding subscriber terminal and method are also presented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a communication system in accordance with the present invention.

FIG. 2 is a block diagram of a subscriber terminal in accordance with the present invention.

FIG. 3 is a block diagram illustrating a decryption hierarchy for use in accordance with the present invention.

FIG. 4 is an on-screen display for a user interface in accordance with the present invention.

FIG. 5 is another on-screen display for a user interface in accordance with the present invention.

FIG. 6 is yet another on-screen display for a user interface in accordance with the present invention.

FIG. 7 is a flowchart illustrating a method for providing digital coupons in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A method and apparatus are presented for allowing users of program services such as pay television to obtain credits when viewing particular programs. The invention enables program service providers to transmit credit information in the form of "digital coupons" to individual subscriber ter-

minals to promote particular programs and reward viewer loyalty. The digital coupons may be generated locally in the terminals based on criteria sent by the service providers, or transmitted directly as an entitlement by the service provider.

FIG. 1 is a block diagram of a communication system in accordance with the present invention. The system includes a transmitting end, shown generally at 110, a channel 120, and a receiving end, shown generally at 130. The transmitting end 110 includes a central controller 130 which communicates with a PPV order processing function 115, a terminal usage pattern data accounting function 125, an encryptor/multiplexer/modulator 150, a digital coupon information function 135, a program service data function 140, and a control data function 145.

The receiving end 130 includes a number of terminals including terminal 1 (160) through terminal N (170), which receive the digital coupon information, program service data, and control data via a hub 124 and path 122. Each terminal has an associated display such as a television for displaying the program service data. For example, "terminal N" 170 has an associated display 180. In the example shown, the terminals 160, . . . , 170 are able to communicate with the PPV order processing function 115 and usage pattern data accounting function 125 via the channel 120.

For example, in a cable television network, such upstream communication may be provided on a channel (e.g., RF spectrum) which is separate from the channels over which the program service data is communicated. A frequency-division multiplexing scheme may be used to achieve this goal. Alternately, a time-division multiplexing scheme may be used, or the terminals 160, . . . , 170 may communicate with the PPV order processing function 115 and usage pattern data accounting function 125 via a separate communication link such as a telephone network. Moreover, as discussed in greater detail below, the present invention can be implemented without the PPV order processing function 115 and/or usage pattern data accounting function 125.

The channel 120 may comprise coaxial cable, optical fiber, and/or a wireless link such as a satellite or RF broadcast link. The transmitting end 110 of the system may be a cable television system headend, a satellite uplink center, or an RF broadcast center, for example.

The digital coupon information function 135 comprises a memory for storing digital coupon information in accordance with the present invention. The digital coupon information is communicated to the terminals 160, . . . , 170 at the receiving end 130 of the system. Furthermore, when the terminals 160, . . . , 170 are addressable, the digital coupon information may be targeted to individual terminals and/or to groups of terminals, for example, according to demographic data. Alternatively, the digital coupon information may be transmitted via a path which is separate from that of the program services.

The digital coupon information provides credits which the terminals can use for a number of purposes. For example, the digital coupon information may provide a discount when the terminals order one or more PPV programs through the PPV order processing function 115. As an example, if a terminal orders five PPV programs within the current billing cycle, the digital coupon credit may allow the terminal to order a sixth PPV program at no charge. Or, for terminals that order PPV programs infrequently, the digital coupon credit may allow the terminal to order a first PPV program at half-price. The digital coupon may be generated automatically based on program coupon criteria established by the service provider.

This has the advantage of requiring no direct involvement by the service provider. This is also suitable for broadcast environments where the return path either does not exist, is slow, or not set-up for interactive transactions.

Alternatively, the digital coupon information may allow the terminals to access premium program services at a reduced charge, or at no charge, or allow the terminals to access other information, such as a software program, a computer game, a book in electronic form, a musical composition, an on-screen television program guide, movie or restaurant reviews, or other promotional, informational or educational material. For example, the digital coupon information may allow a terminal to access a premium movie channel for two days with each PPV purchase, or to download one computer video game, or to gain one hour of free connect time to a computer database.

The term "program service" is thus used herein to encompass television, multimedia, and other audio and/or video signals as well as computer software or virtually any other information that can be accessed by, and/or communicated to, the terminals via the channel 120. The term "credit" is used herein to indicate that the terminals are provided with a benefit such as a reduced or waived charge when accessing and/or obtaining program services via the channel, or for obtaining merchandise via the channel which is delivered to the subscriber by other means (e.g., by mail).

The terminals 160, . . . , 170 do not realize the credit which is offered with the digital coupon information until the terminals satisfy certain preconditions. Each terminal includes means for monitoring various factors which define the terminal's usage pattern data over a defined time period, including, for example, the number of PPV programs purchased, the amount of PPV charges incurred, whether, and for what duration, the terminal has been tuned to a particular program or program service, whether the terminal has recently upgraded to one or more premium program services, and whether a promotional period is in effect. The promotional period may apply to individual terminals, such as those of new subscribers, to selected groups of terminals, or to all terminals.

Accordingly, monitoring means in the terminals monitor the above factors to determine whether the usage pattern of the terminal corresponds with the preconditions of the digital coupon information. Optionally, in a "report-back" function, the usage pattern data is periodically transmitted from the terminals to the usage pattern data accounting function 125, for example, via the hub 124 and channel 120, or, alternatively, via a telephone network. For example, the usage data may be transmitted daily, weekly, or monthly.

Such usage pattern data provides valuable information for program service providers and advertisers which can be used to better target individual subscribers and groups of subscribers with products and services with which they are likely to be interested. Moreover, the usage pattern data allows the interested parties (e.g., promoters and advertisers) to determine the effectiveness of various promotions. For example, when the digital coupon information provides a one-half price PPV program to subscribers who infrequently order PPV, the success rate of the program can be determined from the usage pattern data at the function 125.

As another example, when the digital coupon information provides two free days of access to one of a number of available premium program services, the selected premium program service can be monitored, and the subscriber can be subsequently offered a digital coupon which allows him to upgrade to the selected premium program service, e.g., at

one-half off the normal charge for the first month. Various other marketing strategies may be used with the present invention to enhance revenue and customer goodwill. For example, a subscriber may be given coupon credit for a free pay-per view movie on his birthday.

Moreover, the digital coupon balance may be adjusted according to lotteries or other contests or games. For example, subscribers may be able to enter a lottery for additional coupons if they spend a certain amount of money. Or, the subscriber may play interactive games of chance where the prizes and losses are determined in terms of coupons.

However, even if the usage pattern data is not reported back to the function 125, the monitoring means in the terminal can determine whether the usage pattern data meets the preconditions of the digital coupon information. Preferably, this is done in a secure manner to prevent tampering by pirates, as discussed in further detail below.

The controller 130 causes the digital coupon information from function 135 to be encrypted and multiplexed at the encryptor/mux/modulator 150 along with the program service data from function 140 and the control data from function 145. The program service data may comprise video and/or audio data which is stored locally on storage media, and/or which is received from an external source such as a satellite downlink. Alternatively, the program service data may comprise computer software or other electronic information.

The control data includes cryptographic data which is used for generating working keys at the terminals for decoding the received data. Typically, one or more premium program services are communicated with basic program services over the channel 120. Both the basic and premium program services may be accessed with possession of the appropriate group key or keys. The group key or keys are delivered as part of an Entitlement Management Message (EMM). Possession of the group key or keys along with the appropriate entitlement control data allows the terminals to recover program keys from the program data sent by the service provider in Entitlement Control Messages (ECM).

The program keys allow the derivation or decryption of the working keys which are used to encrypt the programming signal at the uplink or headend side, and to decrypt the program signals on the downlink or consumer decoder side. The term "recover" is used herein to indicate that a program service is received at a terminal and retrieved for use (e.g., display) by the subscriber.

The control data included in an Entitlement Control Message (ECM) is used to control access to a particular program service (i.e., channel). The ECM control data tells the terminal which entitlement needs to be held by the terminal in order to be authorized to access and recover the particular program service. Typically, the ECM message which delivers the control data information is also used to deliver the program key information. The ECM message therefore not only defines program parameters but also delivers a key or precursor key (e.g., pre-key).

The ECM control data may further include data for providing the terminals with the cost for ordering a PPV program. This control data may further indicate the cost, in terms of the number, and type of coupons required to access the program, along with other details listing what number of coupons is required for a discount, and so forth.

FIG. 2 is a block diagram of a subscriber terminal in accordance with the present invention. Like-numbered elements correspond to the elements of FIG. 1. A

demultiplexer/demodulator 205 of the terminal 170 receives the program service data, digital coupon information, and control data from the path 122 and hub 124. Demultiplexing and demodulating is performed using conventional techniques. The encrypted program service data is provided to a decryption processor 212 and a switch 218 via lines 210 and 214, respectively, while the encrypted control data and digital coupon information are provided to a secure processor 220 via line 230.

The encrypted program service is decrypted by the decryption processor 212 to provide a clear signal at output 216 of the decryption processor. The secure processor 220 may receive the decrypted digital coupon information from the decryption processor 212. The decryption processor 212 can utilize a conventional decryption scheme, such as that disclosed in Gilhousen, et al., U.S. Pat. No. 4,613,901 entitled "Signal Encryption and Distribution System for Controlling Scrambling and Selective Remote Descrambling of Television Signals," or Bennett et al., U.S. Pat. No. 4,864,615 entitled "Reproduction of Secure Keys By Using Distributed Key Generation Data," both incorporated herein by reference.

The decryption processor requires working keys (WK) to decrypt the signals input thereto via line 210. The working keys are generated by the secure processor 220 in response to the control signals received via line 230. Firmware for the secure processor is stored in read only memory (ROM) 224. The secure processor 220 is also provided with random access memory (RAM) 222. A secure portion of the RAM 222 holds unit specific keys and/or seeds for use in decryption of a monthly group key, as discussed in greater detail in connection with FIG. 3.

A user interface 226 enables a viewer to select program services for viewing on a television (TV) 180. If a user is authorized to receive the selected service by subscription, individual purchase (e.g., pay per view), or according to a digital coupon credit, the secure processor 220 will actuate the switch 218 to couple the decrypted output 216 from decryption processor 212 to the TV 180 via user interface 226. Otherwise, the user interface and TV will only receive the encrypted signal via line 214 and switch 218. As will be appreciated by those skilled in the art, switch 218 could alternatively be configured to provide a barker channel (e.g., a fixed message) to the user, or no signal at all, in the event that the user is not authorized to access the selected service.

The secure processor 220 monitors the programming which is selected by the user via the user interface 226 to determine whether the user has met the preconditions for obtaining the digital coupon credit. For example, if the digital coupon provides a credit for one free PPV program when five PPV programs are purchased at the regular price, the secure processor will record each occurrence of a purchase of a PPV program. The RAM 222 may be used to store the corresponding data. The usage pattern data thus includes data which is related to the digital coupon preconditions but can include other user selections as well. A communication interface 230 such as a data modem is provided to allow the terminal to transmit buy orders for VOD programming and certain types of programming which require a service provider's authorization for acquisition to the PPV order processing function 115 of FIG. 1. PPV purchases processed locally by the terminal and stored internally to the terminal may be forwarded to the PPV processing function for billing purposes. The interface 230 also allows the terminal 170 to transmit the usage pattern data to the usage pattern data accounting function 125 of FIG. 1.

The terminal receives control data in the form of an Entitlement Management Message (EMM) which provides

an initial currency credit balance for the terminal 170. In this case, when a user orders PPV programs, for example, the overall currency credit balance is decreased by the cost of the programs. The EMM message originating from the service provider may or may not deliver an initial or additional coupon credit to the terminal.

Typically, coupon credit is generated when the preconditions for obtaining the digital coupon credit are realized. The coupon credit balance can be immediately adjusted. As an illustration, assume the initial credit balance is \$40, and each PPV program costs \$5. Then, the credit balance will drop successively to \$35, \$30, \$25, \$20 and \$15 after the first five programs are purchased. At this time, the usage pattern data meets the preconditions of the digital coupon information, and the coupon credit balance gets incremented by one.

Alternatively, the coupon credit balance is incremented by one with each PPV purchase. When the terminal tunes in to the sixth program, the terminal receives a Entitlement Control Message (ECM) for the program. The terminal uses the ECM to determine the different ways that the program may be accessed. The ECM will also describe the currency cost and the coupon cost, if the program is available by coupon. The terminal will automatically determine whether or not the terminal has a coupon or coupons to acquire the program. If so, the program is automatically offered to the viewer, or the viewer is prompted to purchase the program using currency or coupons.

By choosing the coupon option, the next order for a PPV program is provided free, and the coupon credit field is decremented appropriately. Thus, the balance remains at \$15. Alternatively, the terminal is charged for the sixth program, but the secure processor increments the credit balance by the cost, so there is no net change in the credit balance. The secure processor may provide a display on the user interface 226 that informs the viewer that the preconditions of the digital coupon information have been met. Of course, it is possible for coupon credits to accumulate when the corresponding preconditions are met but the credits are not realized, i.e., cashed in. The credits may be retained in the terminal for a predetermined period such as two or three months, or indefinitely. The secure processor may inform the subscriber if the credits are about to expire.

As described in further detail below in connection with FIGS. 4-6, the viewer may query the user interface 226 to determine the credit balance along with other related information.

FIG. 3 is a block diagram illustrating a decryption hierarchy for use in accordance with the present invention. An encrypted program pre-key is input via terminal 340 to a decryption function 344 which also receives a monthly group key via terminal 342. The program pre-key is unique to each encrypted program offering (e.g., television program) that is available for decryption. The group key is changed on a periodic basis, e.g., once each month. The decryption function 344 decrypts the encrypted program pre-key to provide a program pre-key that is used as one input to a one-way function 348. The other input to one way function 348 comprises various program and coupon attributes, including access requirements, such as coupon and currency cost, for the corresponding program. The access requirements must be met to obtain authorization to view the program. The program and coupon attributes are input via terminal 346, and the one way function processes the program pre-key and program attributes to provide a program key.

The program key output from one way function 348 is used as one input to another one way function 352 that also

receives, via terminal 350, an initialization vector (IV) representative of time. The processing of the initialization vector and program key by one way function 352 generates the working keys required by decryption processor 212 of FIG. 2 to decrypt the program service selected by an authorized user. A further description of the generation of the various keys, including working keys (provided in a "keystream"), can be found in the aforementioned Bennett, et al. patent.

Optionally, the digital coupon information and program services can be encrypted according to a common cryptographic key. This could allow an authenticated file, for example, which represents a coupon image, to be sent to the decoders. The coupon could subsequently be redeemed as an authenticated image by transmitting the coupon from the decoder to the program service provider or other accounting center.

FIG. 4 is an on-screen display for a user interface in accordance with the present invention. The display 400 may be invoked as part of a graphical user interface (GUI) which allows a user to select channels and control other features such as volume and the like. Such interfaces are well known in the art. The display 400 may be controlled by a hand-held remote control, a pointing device, voice command or any other available means. For example, a user may select a PPV program such as a movie from a graphical user interface which causes the display 400 to appear.

The display 400 includes a field 410 which informs the user that he is not currently subscribed to the selected program. That is, the user must order the program. A field 420 informs the user that he has different options in ordering the program. Fields 430-460 present the options. A field 440 presents a first option wherein the movie may be purchased as an impulse pay-per-view (IPPV) program with the cost being deducted from an available cash credit balance. The user is thus informed of the cash cost of the movie and the available cash credit balance. The program can be purchased as long as there is a sufficient cash credit balance.

A field 450 presents a second option, where the program may be purchased using digital coupons alone. The user is informed of the coupon cost of the movie and the available coupon credit balance. The program can be purchased as long as there is a sufficient coupon credit balance. The digital coupons are referred to here as "TV" coupons.

A field 460 presents a third option, where the program may be purchased using a combination of cash and digital coupons. The user is informed of the cost of the movie using both coupons and cash, and the available cash credit balance and coupon credit balance. While only one cash/coupon combination is provided in field 460, it will be understood that other combinations may also be provided. In fact, the coupons may be assigned a cash value for this purpose.

In another option, not shown, a subscriber may order a PPV program for a discount if the subscriber is willing to have commercial messages appear which would not otherwise be present. For example, a commercial message using teletext may appear on the bottom portion of the screen when viewing a PPV movie. Or, with VOD, the PPV movie chosen may have periodic commercial message breaks when the discounted program is selected, whereas no commercials would be provided otherwise.

FIG. 5 is another on-screen display for a user interface in accordance with the present invention. Here, the display 500 provides information on the number of coupon credits which have been accumulated while viewing different channels. For example, the various program service providers may

incrementally
Number

DATE
BASE

provide viewers with coupons based on the number of hours of that service provider which is viewed per week, and/or which programs were viewed.

Fields 510 and 530 list the various program service providers, while fields 520 and 540 list the number of coupon credits which have been accumulated. For example, for the service provider Home Box Office (HBO), there is a balance of four coupons. In this manner, the program service providers may compete to encourage viewership. For example, when launching a new program, additional coupons may be provided. Furthermore, coupons may be accumulated based on the time of day or day of week that programs are viewed. Moreover, program service providers that are commonly owned may award coupons to encourage viewership of their programs.

FIG. 6 is yet another on-screen display for a user interface in accordance with the present invention. The display 600 provides an example of the variety of items from which the subscriber may select using the digital coupons of the present invention. Moreover, each of the program service providers along with other interested parties may offer their own items. A field 610 indicates that the particular display 600 is that of the service provider Cable News Network (CNN). A field 620 indicates the current coupon credit balance, while a field 630 indicates the items that may be obtained, and field 640 indicates the number of coupons needed to obtain each item.

Thus, the user may redeem the digital coupons for a wide variety of items, including additional programming that can be communicated to, or accessed by, the terminal as well as non-programming items which can be delivered to the user's home, e.g., by mail.

Some items may not require any digital coupons. For example, a field 650 describes product information which can be communicated to the subscriber's terminal or delivered to the subscriber's home at no cost. However, when the subscriber requests the product information, the usage pattern data is updated and may be subsequently provided to the usage pattern data accounting function 125 of FIG. 1, where it may be used for marketing purposes.

FIG. 7 is a flowchart illustrating a method for providing digital coupons in accordance with the present invention. The flowchart describes an embodiment where an initial cash credit balance is provided to a terminal, for example, on a monthly basis. Then, when the user desires to view programming such as PPV programming that has an associated cost, the cost is deducted from the cash credit balance. Furthermore, when the user meets the preconditions of the digital coupon information as determined by the usage pattern data, a coupon credit balance is accumulated. The coupon credit balance may be used to purchase additional program services in lieu of cash, or, optionally, to defray the cost of programs already purchased. In the latter case, the coupon credits may be assigned a cash value.

At block 705, the controller at the transmitter delivers an initial cash credit balance to the terminals. The amount delivered to each terminal may be different and may be based, for example, on past purchasing habits. At block 710, the controller delivers the digital coupon information to the terminals. Again, different terminals may receive different coupon data according to demographic factors and the like. At block 720, the terminal usage pattern is monitored and recorded. In particular, events which meet the preconditions of the digital coupons are recorded, while other data indicative of user habits may also be recorded.

The digital coupon preconditions may account for a variety of events, such as whether the subscriber has pur-

chased a given number N of PPV programs in the last M days (block 722), in which case a digital coupon credit "1" is awarded at block 724. It will be appreciated that different types and amounts of coupons may be awarded according to the particular precondition which the viewer meets. For example, some coupon credits may be more valuable than others, or may be redeemed for different benefits.

At block 726, if it is determined that the subscriber has purchased X\$ of PPV programs in the last Y days, a digital coupon credit "2" is awarded at block 728. At block 730, if the subscriber has viewed an "infomercial" for a number Z minutes, a digital coupon "3" is awarded at block 732. An "infomercial" is a commercial message that has the length and format of a regular program, e.g., such as one-half hour or more, and generally garners a relatively small audience. For marketing purposes, it is desirable to reward viewers for viewing infomercials even though there is no charge incurred for viewing the program. Optionally, coupon credit may be awarded only for the first viewing of the program, so additional coupon credits are not awarded for repetitive viewing of the same program.

At block 734, if the subscriber has upgraded from a basic programming tier to a premium programming tier, or to a higher premium programming tier, a digital coupon "4" is awarded at block 736. At block 738, if a promotional period is in progress, a digital coupon "5" is awarded at block 740. Such a promotional period would generally apply to all subscribers.

At block 750, the total amount of coupon credits is determined. At block 760, if the coupon credit balance is above zero, then at block 770, the user is prompted by the user interface (e.g., every time the television is turned on) to select among the various options which are available in redeeming the digital coupons. For example, the subscriber may order PPV programming for a discount or no charge, access premium programming for a predetermined period of time, or simply pass and take advantage of the available options at another time. The various options have been discussed above in greater detail in connection with FIGS. 4-6. In addition to the periodic prompts described above, a user will also have the capability of accessing the coupon redemption menu at any time via the remote control.

At block 780, the digital coupon balance is adjusted by the number of coupons redeemed at block 770, and the monitoring of the terminal usage pattern continues at block 720.

Note that it is possible to verify that the user is actually viewing a particular program by requiring some sort of subscriber involvement. For example, to verify that a subscriber has watched an infomercial for Z minutes, the terminal may require the subscriber to input a command to the user interface. The user interface may provide a message such as "Do you wish to continue", to which the subscriber must respond to meet the digital coupon preconditions. An internal timer within the terminal may be halted until a response is received.

For subscribers who view infomercials and the like, to ensure that only one set of coupons are awarded per program, the COUPON_RECORD_DURATION field as discussed below in Table 3 is provided to indicate a duration in which the program record of the infomercial is stored in the terminal. This precludes the same subscriber from getting repeated coupons for the same infomercial that is run again and again, while still enabling the same program ID for the infomercial to be used repeatedly.

The data delivery syntax set forth below in Tables 1-4 may be used in accordance with the present invention.

13

Tables 1-3, respectively, describe data fields which may be used when digital coupons are delivered to terminals using an EMM, an IPPV ECM purchase linkage, and a program re-key ECM. Table 4 describes data fields which may be used with all delivery methods. It should be appreciated that the syntax shown is for illustration only and that other data delivery schemes may be substituted.

TABLE 1

Syntax	Size	Description
COUPON_PROVIDER_ID	3 bytes	Identifies coupon sponsor
NEW_COUPON_CREDIT	3 bytes	Absolute number of coupons for service provider in a month
NEW_COUPON_DEBIT	3 bytes	Absolute debit for service provider in a month
COUPON_CREDIT	3 bytes	Total accrued coupons
COUPON_SEQ_NUMBER	1 byte	Epoch (time period) of coupon delivery

TABLE 2

Syntax	Size	Description
COUPON_PROVIDER_ID	3 bytes	Identifies coupon sponsor
COUPON_CREDIT	1 byte	Coupon credit remaining

TABLE 3

Syntax	Size	Description
COUPON_ID	2 bytes	COUPON_ID + COUPON_PROVIDER_ID = unique coupon ID)
COUPON_PAYOUT_DURATION	2 bytes	Time period subscriber must view program to obtain coupon credit
COUPON_RECORD_DURATION	3 bytes	Time period coupon is retained at terminal
COUPON_PROVIDER_ID	3 bytes	Identifies coupon sponsor

TABLE 4

Syntax	Size	Description
COUPON_DEBIT	2 bytes	Number of accrued coupon debits
COUPON_PACKAGE_ID	2 bytes	Type of coupon for package program
IPPV_CREDIT	2 bytes	Cash credit balance for pay-per-view
PACKAGE_PROVIDER_ID	2 bytes	Identifies service provider of package of programs
PKG_COST	1 byte	Cash charge for package program
PKG_ID	1 byte	Identifies package
PROGRAM_PAYOUT_DURATION	1 byte	Minimum time subscriber must view program to gain credit
PROGRAM_INFORMATION	2 bytes	Video/audio data of program
SHOW_COUNT	2 bytes	Count of shows purchased
VH_LIMIT	2 bytes	View History Limit before report back is mandatory
VIDEO PROVIDER ID	2 bytes	Identifies service provider

To thwart piracy, digital coupons may only be offered to subscribers with established impulse PPV accounts where there is a report-back capability. This can be effected, for example, by using a bit as a flag in either the group re-key EMM or Program re-key ECM.

14

The report-back feature discussed above in connection with the usage pattern data accounting function 125 of FIG. 1 allows the program service providers and network controller to monitor the audience size for different programs. The use of digital coupons can therefore allow the service providers to detect viewership patterns over a wide cross-section of programs, and not just premium shows. In other words, shows which are not available through PPV might be made available through coupons.

In the following program delivery scenarios, it is assumed that a real channel (i.e., program) must exist which can be purchased with coupons. This can be enforced by hashing the program information to generate a program key as explained further below. Therefore, a program cannot be viewed using digital coupons unless it is actually offered to coupon holders.

However, pirates may attempt to tamper with the delivery of the coupons. The main objective of the pirate is to defeat the system by providing false messages (e.g., "spoofing") to obtain digital coupons without having to perform any of the coupon preconditions. In accordance with the present invention, different ways to securely deliver the COUPON_CREDIT field to terminals are discussed.

There are three ways to deliver the digital coupons, i.e., using a group re-key EMM, an IPPV purchase linkage, or a program re-key ECM. The group re-key message technique can handle a distribution of coupons to a general population of terminals as well as providing a method that is linked to IPPV purchases. IPPV purchase linkage could be done independently from group re-key message delivery, however. The delivery of coupons via the group re-key message may be mutually exclusive from the program re-key technique since, with the program re-key technique, the network controller or PPV order processing center does not know how many coupons a subscriber might earn using the method where the coupons are generated internally by the terminal. Thus, management of group re-key based coupons cannot be handled as securely inside a terminal unless group re-key based coupons are tracked separately from program re-key based coupons.

Direct delivery of coupons through a group re-key entitlement management message (EMM) is the most straightforward way to control the delivery of coupons to subscribers. This approach is suitable for IPPV service providers who decide to reward particular subscribers based, for example, on previous purchasing volume. The service provider thus knows which particular subscribers are to receive the digital coupons and can therefore direct a unit specific EMM to each of the subscribers.

Additionally, the group re-key EMM approach is suitable for providing subscribers with digital coupons along with a designator which allows text message commercials. These on-screen displays convey advertising and can be overlaid on top of the video and audio displayed. As discussed previously, these subscribers are willing to view such commercials to obtain digital coupon benefits such as discounts on other programs. Again, the service providers know exactly which subscribers agreed to have text message commercials delivered to them, and can therefore provide them with the corresponding digital coupons through an EMM.

Moreover, using the COUPON_CREDIT and VH_LIMIT data fields, individual service providers can send digital coupons to individual subscribers. Each service provider is identified by the field VIDEO_PROVIDER_ID. If a pirate were to synthesize a group key message with a

15

false VIDEO_PROVIDER_ID and COUPON_CREDIT, thereby resulting in a bad group key, the pirate might be able to create false VIDEO_PROVIDER_ID, COUPON_CREDIT pairs inside the terminal.

One solution to the above problem is implemented using EMM authentication. In particular, if the group re-key EMM used by a transmitting satellite, for example, is hashed. The hash is then encrypted to create a signature. A pirate cannot produce a counterfeit group re-key EMM without knowledge of a terminal's unit keys, and the key hierarchy. In this case, the counterfeit message will be rejected without processing. Another way to authenticate a message is to use public key cryptography to sign or encrypt the entire message. This can also prevent the generation of counterfeit messages.

Furthermore, a pirate may use "replay" attacks using legitimately built messages. In this case, a legitimate message is saved and provided to a terminal months after the message was originally created and first used to make new COUPON_CREDIT inside the terminal. To protect against this, group sequence numbers may be incremented.

Moreover, the pirate may attempt to replay the message in the same month that it was generated. To protect against this, new COUPON_CREDIT could be tracked during a particular month. At the end of the month, it can be added to COUPON_CREDIT that was earned in previous months. When the COUPON_CREDIT FIELD is sent to the terminal during the month in the group re-key EMM, it would be the absolute coupon credit issued to a particular terminal. Moreover, an additional field, COUPON_DEBIT, may be created inside the terminal to manage the coupons from a particular service provider for that month. Another way to secure against replay attacks within the same month would be to sequence the EMMs themselves. The decoder may then be able to differentiate between a new message and one that it has seen before. Another method would be to include a date/time parameter in the EMM. As with a sequence number, this field can only go forward or stay the same, but cannot be changed to a past value.

For each individual service provider, any new COUPON_CREDIT value must be authenticated, e.g., in the group re-key message just as with the COUPON_CREDIT and VH_LIMIT fields since merely signing the message or using public key cryptography will not prevent such replay attacks. Moreover, each new coupon record should track the sequence number which indicates when it was generated. When the group key epoch occurs, the group re-key EMM that was originally used to create the coupon record will not be able to create additional coupons since the message will be old. At that time, the new COUPON_CREDIT can be added to old COUPON_CREDIT. If, during the next month, no new coupons are sent to the terminal, and all of the existing coupons are used, then the entire coupon record can be erased.

In a second digital coupon delivery method, coupons are delivered through an IPPV buy linkage. With each IPPV purchase, a bit in the program re-key message allows a service provider to deliver one or more coupons automatically and instantly to subscribers without waiting to get a report back or performing a "trip" (e.g., delivery) with coupons as in the group re-key method discussed above. If a subscriber did not have any coupons from a particular service provider before, a new service provider coupon record is made. The coupon creation process is therefore tightly linked to actual purchases of IPPV programs. After a number of coupons have been accrued, the subscriber can

16

redeem them. Typically, a service provider will offer digital coupons which can be redeemed only for that service provider's programs. However, groups of service providers may collaborate to provide interchangeable coupons if desired.

In another possible pirate attack, a pirate may attempt to manipulate the number of coupons which are awarded when performing the digital coupon preconditions, e.g., such as purchasing a number of IPPV programs. One possible solution uses a DES hash with encryption (e.g., signature) or public key encryption of the program re-key message. If the number of coupons is authenticated in the IPPV report-back, then the pirate's manipulation of this field would cause a bad cryptographic field.

If the pirate does know the group key, counterfeiting could occur but may be detectable if the view history information (e.g., usage pattern data) is used to hash the coupon value and is sent along in the report-back.

Moreover, if public key cryptography was used in the delivery of the program re-key message, then, even if the pirate knew the group public key, a message still could not be synthesized since the group private key would not be known. Public key cryptography has a distinct advantage over secret key cryptography since the group encrypt or private key is not in the terminal. Consequently, VLSI probing and other attacks against the terminal cannot reveal the key.

In a third delivery method in accordance with the present invention, digital coupons are delivered in conjunction with extended commercial programs known as "infomercials." Preferably, a subscriber is rewarded with digital coupon credits only after viewing the program for a specific amount of time. Furthermore, to prevent the subscriber from simply tuning in the program and walking away, it might be advantageous to require some sort of subscriber involvement such as a control input which is requested by the user interface.

A pirate may be able to alter code in a non-secure processor to automatically provide the subscriber involvement control signal. However, the amount of time that the program must be viewed, or at least tuned in, can be secured. To do this, there is no need to track the maximum time that the program lasts since the infomercial service provider is essentially paying the subscriber to view the program. The PROGRAM_PAYOUT_DURATION field can be loaded into a countdown timer to enforce the minimum viewing time requirement of the digital coupon preconditions. The coupons are thus issued when the timer counts down to zero, and the timer counts down only when the infomercial channel is tuned in. Essentially, this ties up the terminal to tune in the infomercial and precludes it from tuning in another channel.

Furthermore, the COUPON_RECORD_DURATION field is required to determine when the program record should be expunged from the secure processor's memory.

A pirate may attempt to manipulate the field in the program re-key ECM, which indicates how many coupons are to be awarded when viewing the infomercial. One possible solution is to use a DES hash (e.g., signature) or public key encryption of the program re-key message. Like the other attacks described above, signing the program re-key message makes it hard for the pirate to counterfeit the program re-key message without knowledge of the group secret key or private key. Moreover, if public key cryptography is used in the delivery of the program re-key message, then, even if the group public key was known by a pirate, a

Time limit

message could not be synthesized since the group private key is not known.

In another possible pirate attack, the pirate records legitimate program messages, and repeatedly plays back the messages to the terminal. The pirate may modify the terminal to provide control inputs directly to the chip or via the user interface to increase the number of coupons held by the chip. One solution to this attack is to create and store a program record in memory. In particular, the COUPON_CREDIT field is used to authenticate the number of coupons being awarded. In addition to COUPON_PKG_ID and COUPON_PROVIDER_ID, two duration timers are needed instead of one. One timer, COUPON_PAYOUT_DURATION, tracks how long the subscriber must be tuned to the program before coupons are awarded, and the other time, COUPON_RECORD_DURATION, tracks when the program record can be expired from memory. The amount of time that a record should be retained might be two months, for example.

Delivery of program re-key messages by public key is a safer mechanism. A pirate would need to cryptographically search for the group private key to alter program re-key messages. The group private key is not delivered to any terminal anywhere in the network. The length of the group public keys delivered could expand according to the perceived piracy threat. And, the group public and private keys may be changed through the delivery of new EMMs. If there is a system breach, the infomercial feature could be abandoned simply by making program re-key ECMs with the coupon issuing feature missing, or not allowing IPPV purchases with coupons.

In the above discussion, it was seen that there are three distinct methods for delivering coupons to the terminals. The first is group re-key EMM based, the second is tightly tied to IPPV authentication, and the third is Program Re-key ECM based using the "infomercial" concept.

The group re-key method is similar to how IPPV is implemented with the only absolute COUPON_CREDIT given, and requiring a COUPON_DEBIT field to exist inside the terminal for each service provider with a COUPON_PROVIDER_ID.

The IPPV purchase linkage method is a hybrid between the group re-key method and the program re-key method since it takes advantage of IPPV authentication that is already done and securely authenticated inside the terminal, and yet is delivered by a program re-key ECM with the appropriate parameters set. Coupons using this method can only be delivered through a real IPPV purchase.

With the program re-key method, coupon redemption may or may not be tied to the view history report-back. For auditing of viewership, coupon redemption is tied to the report-back since a communication link such as a telephone network is required.

Accordingly, it can be seen that the present invention provides a system for transmitting digital coupons to subscriber terminals for various promotional purposes. By delivering and managing the coupons electronically, the coupons are more likely to be used by the subscribers, and distribution and handling costs for the promoters are significantly reduced. Subscriber loyalty can be rewarded, while subscribers can also be selectively targeted to try out programming in which they are likely to have a special interest. Subscribers can be even be encouraged to view commercial programming such as infomercials. Additionally, with an optional report back feature, terminal usage pattern data can be retrieved and analyzed to deter-

mine the effectiveness of the promotions and to gather additional demographic and individual data. Furthermore, the integrity of the scheme can be assured with various encryption techniques.

Although the invention has been described in connection with various specific embodiments, those skilled in the art will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims.

For example, accounting of the coupon credit balance may be maintained by the network controller or other entity apart from the terminal. This accounting may be updated real-time as the coupon balance changes, or periodically, such as where an automatic telephone report back capability is provided.

What is claimed is:

1. A transmitting end apparatus of a subscriber television network, comprising:

a programming services data function for providing programming services;

a digital coupon information function for providing digital coupon information; and

a controller; wherein:

said controller is responsive to said programming services function for transmitting the programming services to a plurality of subscriber terminals of the network via a communication channel;

said programming services are adapted to be recovered by said subscriber terminals;

said controller is responsive to said digital coupon information function for delivering the digital coupon information to said terminals via said communication channel;

said digital coupon information defines preconditions for enabling said terminals to obtain credits when recovering the programming services; and
said digital coupon information enables the terminals to maintain a running credit balance according to credits obtained and credits redeemed.

2. The apparatus of claim 1, wherein:

the credits are redeemable by users at the respective terminals for obtaining programming services at a reduced charge.

3. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals recover particular programming services to obtain credits.

4. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals recover a specified number of the programming services to obtain credits.

5. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals recover the programming services for a specified duration to obtain credits.

6. The apparatus of claim 1, wherein:

the preconditions require that the respective terminals incur a specified amount of charges in recovering the programming services to obtain credits.

7. The apparatus of claim 1, further comprising:

encryption means operatively associated with said controller for encrypting said digital coupon information and said programming services, prior to transmission to the terminals, according to a common cryptographic key.

19

8. The apparatus of claim 1, wherein:
said digital coupon information function provides different digital coupon information for different ones of the terminals.
9. The apparatus of claim 8, further comprising:
a usage pattern accounting center operatively associated with said controller, and adapted to receive usage pattern data from the terminals; wherein:
said digital coupon information function is responsive to said usage pattern accounting center and said usage pattern data for providing the different digital coupon information.
10. The apparatus of claim 9, wherein:
the usage pattern data indicates a viewing history of the programming services at the terminals over a specified time period.
11. The apparatus of claim 1, wherein:
the controller transmits data to the terminals via the communication channel for establishing an initial credit balance at the terminals.
12. A transmitting end method for a subscriber television network, comprising the steps of:
providing programming services and digital coupon information at the transmitting end; and
transmitting the programming services and the digital coupon information from the transmitting end to a plurality of subscriber terminals of the network via a communication channel; wherein:
the programming services are adapted to be recovered by the subscriber terminals;
the digital coupon information defines preconditions for enabling the terminals to obtain credits when recovering the programming services; and
the digital coupon information enables the terminals to maintain a running credit balance according to credits obtained and credits redeemed.
13. The method of claim 12, wherein:
said credits are redeemable by users at the respective terminals for obtaining programming services at a reduced charge.
14. The method of claim 12, wherein:
the preconditions require that the respective terminals recover particular programming services to obtain credits.
15. The method of claim 12, wherein:
the preconditions require that the respective terminals recover a specified number of the programming services to obtain credits.
16. The method of claim 12, wherein:
the preconditions require that the respective terminals recover the programming services for a specified duration to obtain credits.
17. The method of claim 12, wherein:
the preconditions require that the respective terminals incur a specified amount of charges in recovering the programming services to obtain credits.
18. The method of claim 12, comprising the further step of:
encrypting said digital coupon information and said programming services at the transmitting end, prior to transmission to the terminals, according to a common cryptographic key.
19. The method of claim 12, comprising the further step of:
providing different digital coupon information for different ones of the terminals.

20

20. The method of claim 19, comprising the further step of:
receiving usage pattern data from the terminals at the transmitting end; wherein:
the different digital coupon information is provided in response to the usage pattern data.
21. The method of claim 20, wherein:
the usage pattern data indicates a viewing history of the programming services at the terminals over a specified time period.
22. The method of claim 12, comprising the further step of:
transmitting data from the transmitting end to the terminals via the communication channel for establishing an initial credit balance at the terminals.
23. A subscriber terminal in a subscriber television network, comprising:
means for recovering programming services and digital coupon information from a transmitting end of the network via a communication channel;
means for processing said digital coupon information to determine preconditions thereof for enabling the terminal to obtain credits when recovering the programming services; and
means for maintaining a running credit balance according to credits obtained and credits redeemed.
24. The terminal of claim 23, wherein:
said credits are redeemable by a user at the terminal for obtaining programming services at a reduced charge.
25. The terminal of claim 23, wherein:
the preconditions require that the terminal recover particular programming services to obtain credits.
26. The terminal of claim 23, wherein:
the preconditions require that the terminal recover a specified number of the programming services to obtain credits.
27. The terminal of claim 23, wherein:
the preconditions require that the terminal recover the programming services for a specified duration to obtain credits.
28. The terminal of claim 23, wherein:
the preconditions require that the terminal incur a specified amount of charges in recovering the programming services to obtain credits.
29. The terminal of claim 23, wherein:
the digital coupon information is customized for the terminal.
30. The terminal of claim 23, further comprising:
monitoring means for monitoring a usage pattern of the terminal to determine if said preconditions have been satisfied; wherein:
said maintaining means is responsive to said monitoring means for maintaining said running credit balance.
31. The terminal of claim 30, further comprising:
a communication interface for communicating data indicative of said usage pattern from said monitoring means to a usage pattern accounting center at the transmitting end; wherein:
said usage pattern data enables the transmitting end to customize the digital coupon information provided to the terminal.
32. The terminal of claim 30, wherein:
the usage pattern indicates a viewing history of the programming services at the terminal over a specified time period.

21

33. The terminal of claim 23, wherein:
 said maintaining means is adapted to establish an initial credit balance in response to data received from the transmitting end.

34. The terminal of claim 23, further comprising: 5
 a user interface for enabling the terminal to redeem said credits according to a user input.

35. The terminal of claim 23, wherein said digital coupon information and said programming services are encrypted at the transmitting end according to a common cryptographic key, further comprising: 10
 decryption means for decrypting said digital coupon information and said programming services.

36. The terminal of claim 35, further comprising: 15
 authentication means for cryptographically authenticating said digital coupon information.

37. The terminal of claim 36, wherein:
 said authentication means authenticates said digital coupon information according to a group key. 20

38. The terminal of claim 36, wherein:
 said authentication means authenticates said digital coupon information according to a public key.

39. The terminal of claim 23, wherein: 25
 said programming services include programs which are encrypted according to associated program re-keys; and

at least a particular one of said program re-keys is transmitted to the terminal from the transmitting end to allow the terminal to decrypt and recover the associated program using said program re-key; and 30
 said digital coupon information is transmitted to the terminal with said program re-keys.

40. A data processing method for a terminal in a subscriber television network, comprising the steps of: 35
 recovering programming services and digital coupon information from a transmitting end of the network via a communication channel;

processing said digital coupon information to determine preconditions thereof for enabling the terminal to obtain credits when recovering the programming services; and 40
 maintaining a running credit balance according to credits obtained and credits redeemed.

41. The method of claim 40, wherein: 45
 said credits are redeemable by a user at the terminal for obtaining programming services at a reduced charge.

22

42. The method of claim 40, wherein:
 the preconditions require that the terminal recover particular programming services to obtain credits.

43. The method of claim 40, wherein:
 the preconditions require that the terminal recover a specified number of the programming services to obtain credits.

44. The method of claim 40, wherein:
 the preconditions require that the terminal recover the programming services for a specified duration to obtain credits.

45. The method of claim 40, wherein:
 the preconditions require that the terminal incur a specified amount of charges in recovering the programming services to obtain credits.

46. The method of claim 40, wherein:
 the digital coupon information is customized for the terminal.

47. The method of claim 40, comprising the further step of:
 monitoring a usage pattern of the terminal to determine if said preconditions have been satisfied; wherein:
 said maintaining step is responsive to said monitoring step.

48. The method of claim 47, comprising the further step of:
 communicating data indicative of said usage pattern from the terminal to a usage pattern accounting center at the transmitting end; wherein:
 said usage pattern data enables the transmitting end to customize the digital coupon information provided to the terminal.

49. The method of claim 47, wherein:
 the usage pattern indicates a viewing history of the programming services at the terminal over a specified time period.

50. The method of claim 40, comprising the further step of:
 establishing an initial credit balance in response to data received from the transmitting end.

51. The method of claim 40, comprising the further step of:
 receiving a user input to redeem the credits.

* * * * *



US006157719A

United States Patent [19]

Wasilewski et al.

[11] **Patent Number:** 6,157,719[45] **Date of Patent:** *Dec. 5, 2000[54] **CONDITIONAL ACCESS SYSTEM**

[75] **Inventors:** Anthony J. Wasilewski, Alpharetta;
Howard G. Pinder, Norcross; Glendon
L. Akins, III, Gainesville; Michael S.
Palgon, Atlanta, all of Ga.

[73] **Assignee:** Scientific-Atlanta, Inc., Norcross, Ga.

[*] **Notice:** This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] **Appl. No.:** 09/126,921

[22] **Filed:** Jul. 31, 1998

Related U.S. Application Data

[63] Continuation-in-part of application No. 08/767,535, Dec. 16, 1996, Pat. No. 6,005,938, and a continuation-in-part of application No. 08/415,617, Apr. 3, 1995, Pat. No. 5,742,677, and a continuation-in-part of application No. 08/580,759, Dec. 29, 1995, Pat. No. 5,870,474, and a continuation-in-part of application No. 09/111,958, Jul. 8, 1998, abandoned.

[60] Provisional application No. 60/007,962, Dec. 4, 1995, and provisional application No. 60/054,578, Aug. 1, 1997.

[51] **Int. Cl.⁷** H04N 7/167

[52] **U.S. Cl.** 380/21; 380/21; 380/49

[58] **Field of Search** 380/20, 21, 44,
380/49

[56] **References Cited****U.S. PATENT DOCUMENTS**

Re. 33,189	3/1990	Lee et al. .	
4,358,672	11/1982	Hyatt et al. .	
4,405,829	9/1983	Rivest et al. .	
4,531,020	7/1985	Wechselberger et al. .	
4,613,901	9/1986	Gilhousen et al.	380/20
4,634,807	1/1987	Chorley et al. .	
4,736,422	4/1988	Mason	380/20
4,823,385	4/1989	Hegendorfer .	
4,864,615	9/1989	Bennett et al. .	
4,887,296	12/1989	Horne	380/21

4,912,762	3/1990	Lee et al. .	
5,029,207	7/1991	Gammie	380/10
5,124,117	6/1992	Tatebayashi et al. .	
5,231,665	7/1993	Auld et al. .	
5,237,610	8/1993	Gammie et al. .	
5,249,230	9/1993	Mihm, Jr. .	
5,270,822	12/1993	Choi .	
5,282,248	1/1994	DeJoy .	
5,341,425	8/1994	Wasilewski et al. .	
5,381,481	1/1995	Gammie et al.	380/49
5,400,401	3/1995	Wasilewski et al. .	
5,402,490	3/1995	Mihm, Jr. .	
5,420,866	5/1995	Wasilewski .	
5,440,633	8/1995	Augustine et al. .	
5,473,692	12/1995	Davis .	
5,481,542	1/1996	Logston et al. .	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

97/04553 2/1997 WIPO .

OTHER PUBLICATIONS

ISO/IEC 31818-1, Information Technology—Generic Coding of Moving Pictures and Associated Audio: Systems, Draft Nov. 13, 1994.

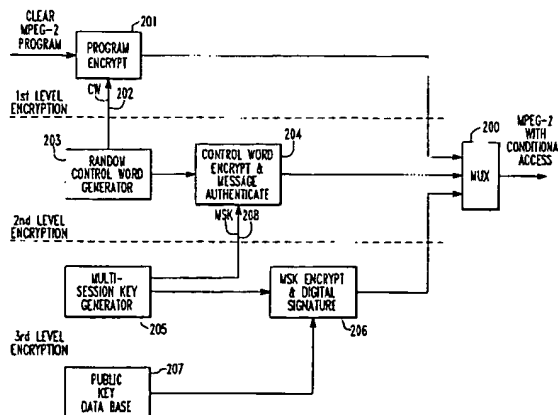
(List continued on next page.)

Primary Examiner—Gilberto Barrón, Jr.

Attorney, Agent, or Firm—Kenneth M. Massaroni; Hubert J. Barnhardt, III; Kelly A. Gardner

[57] **ABSTRACT**

A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

46 Claims, 21 Drawing Sheets

U.S. PATENT DOCUMENTS

5,481,613 1/1996 Ford et al. .
 5,524,052 6/1996 Augustine et al. .
 5,557,678 9/1996 Ganesan .
 5,557,765 9/1996 Lipner et al. .
 5,559,889 9/1996 Easter et al. .
 5,563,950 10/1996 Easter et al. .
 5,568,552 10/1996 Davis .
 5,583,939 12/1996 Chang et al. .
 5,742,677 4/1998 Pinder et al. .

OTHER PUBLICATIONS

ISO/IEC JTC1/SC29/WG11, "Universal Multi-Program Multiplex and Transport for MPEG-2 Systems", Jan. 1993.
 ISO/IEC JTC1/SC29/WG11, "An MPEG-2 Multi-Program Multiplex Syntax", Jan. 1993.
 ISO/IEC JTC1/SC29/WG11, "Requirements and Method for High-Level Multiplexing of MPEG and Other Digital Service Bitstreams with Universal Transport Layer", Nov. 1992.
 FIPS PUB 140-1, "Security Requirements for Cryptographic Modules", Jan. 11, 1994.
 FIPS PUB 74, "Guidelines for Implementing and Using the NBS Data Encryption Standard", Apr. 1, 1984.

FIPS PUB 46-2, "Data Encryption Standard", Dec. 30, 1993.
 FIPS PUB 171, "Key Management Using ANSI X9.17", Apr. 27, 1992.
 FIPS PUB 81, "DES Modes of Operation", Dec. 2, 1980.
 EBU Technical Review No. 266, "Functional Model of a Conditional Access System", Winter 1995/96.
 Whitfield, Diffie, "Authentication and Authenticated Key Exchanges", *Designs, Codes and Cryptography An International Journal*, vol. 2, No. 2, Jun. 1992, pp. 107-125.
 Schneier, Bruce, "Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C", pp. 357-363.
 Menezes, Alfred J., "Handbook of Applied Cryptography", pp. 506-525.
 TM-1244 Rev. 4, "Final Technical Report of the Conditional Access Specialist Group", Nov. 17, 1994.
 Van Schooneveld, D., "Standardization of Conditional Access Systems for Digital Pay Television," *Philips Journal of Research*, vol. 50, No. 1/2, Jul. 1996, pp. 217-225.
 Angebaud, D. and Giachetti, J.L., "Conditional Access Mechanism for All-Digital Broadcast Signals," *IEEE Transactions on Consumer Electronics*, vol. 38, No. 3, Aug. 1992, pp. 188-194.

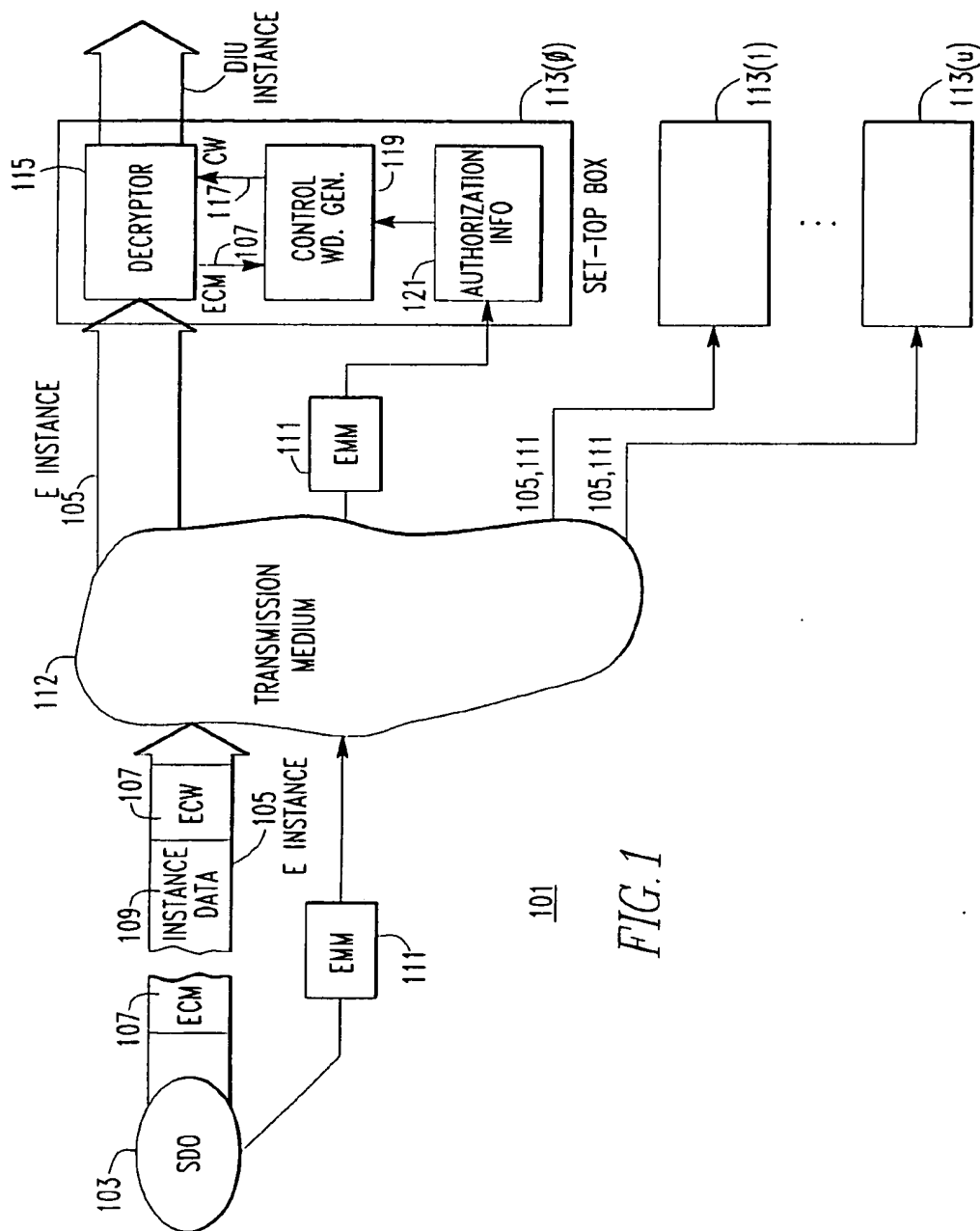
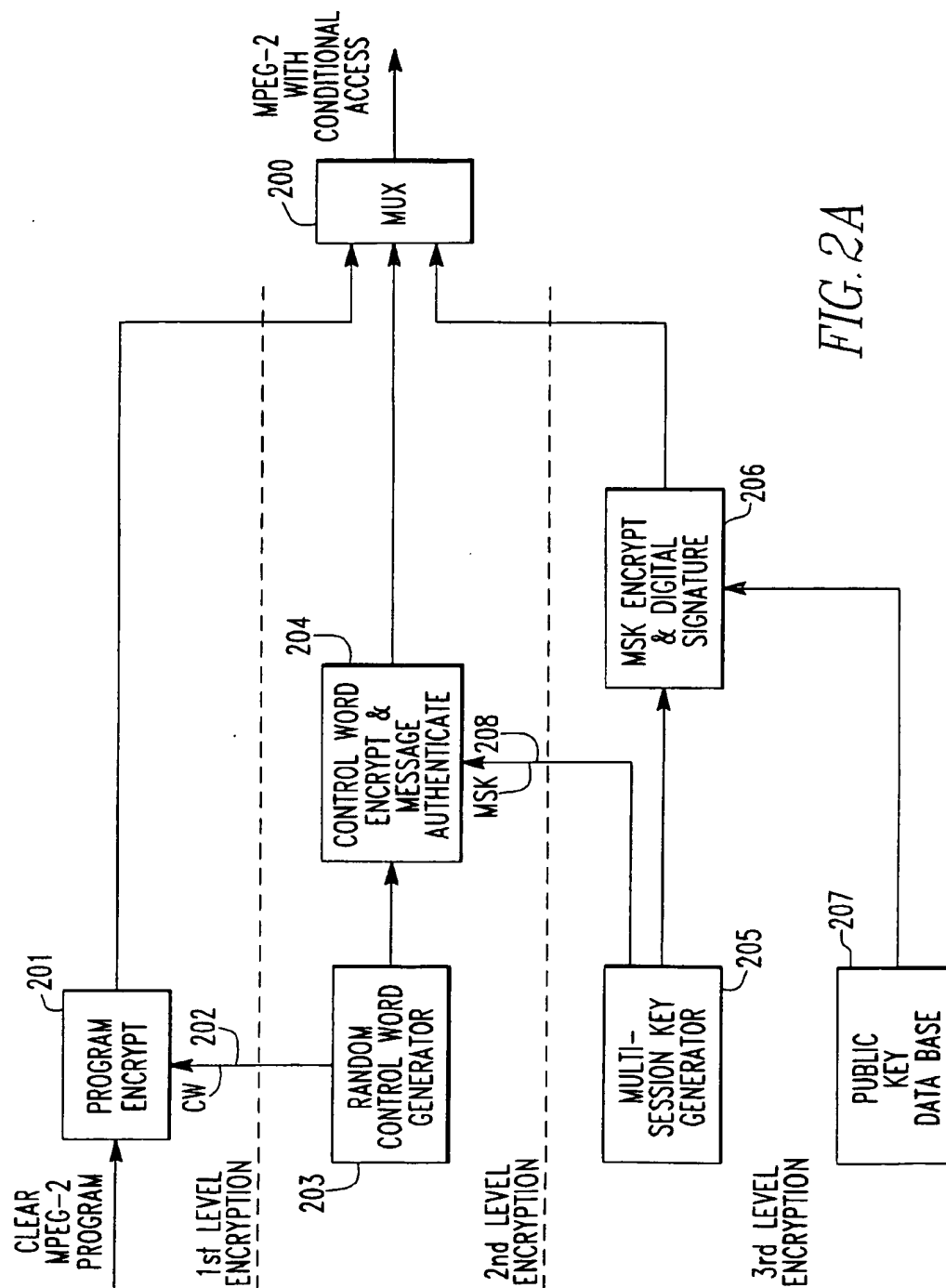
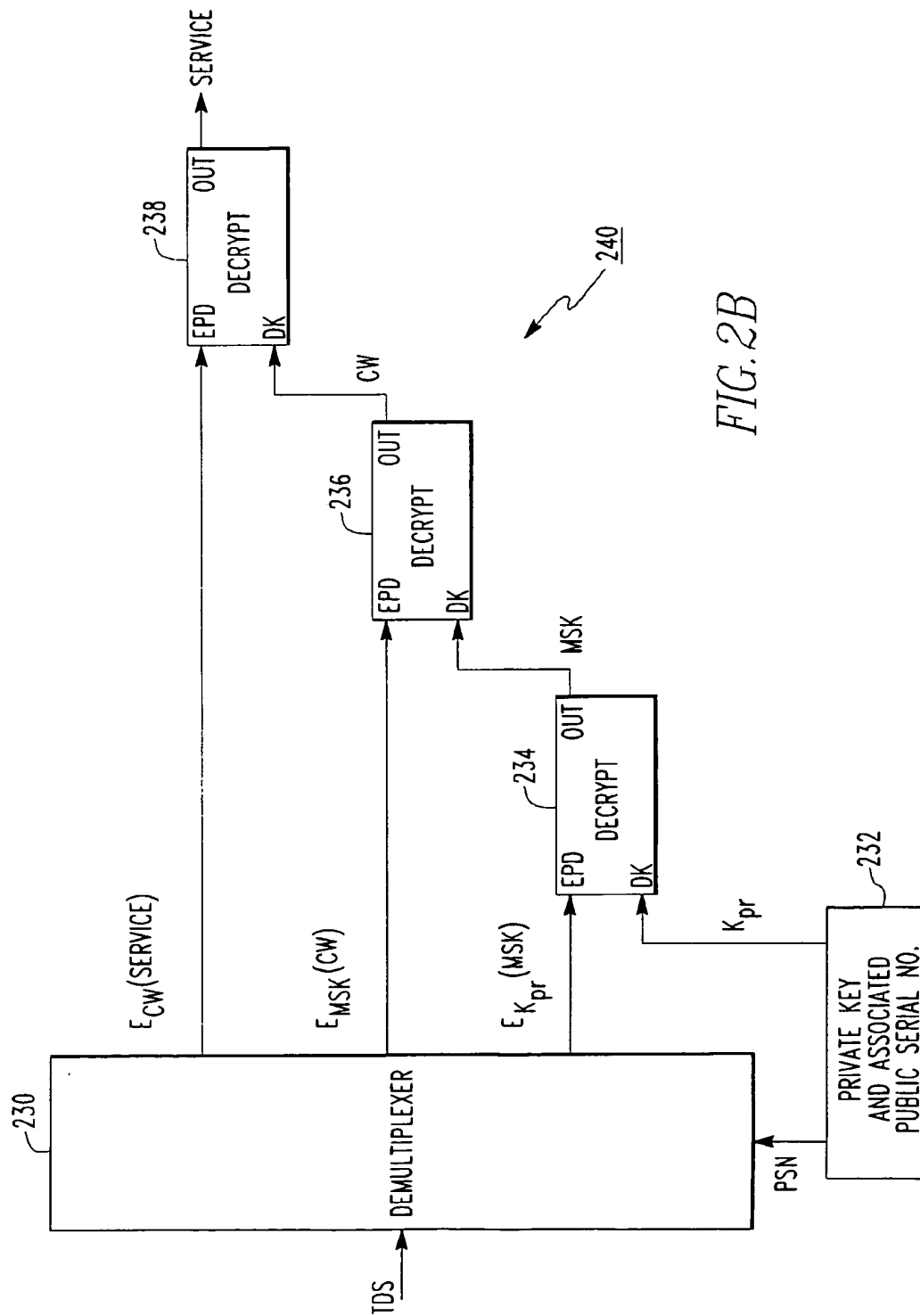


FIG. 1





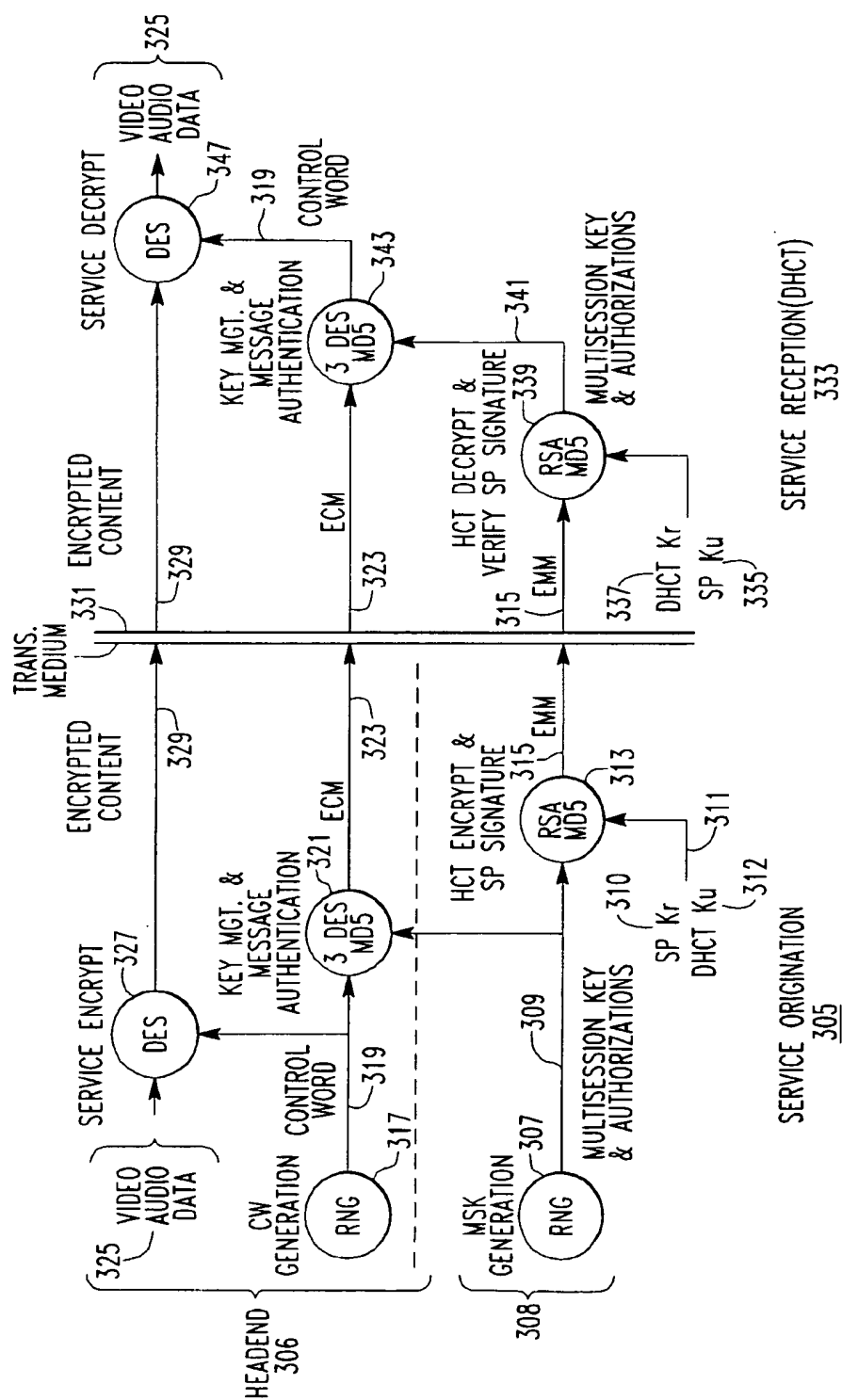
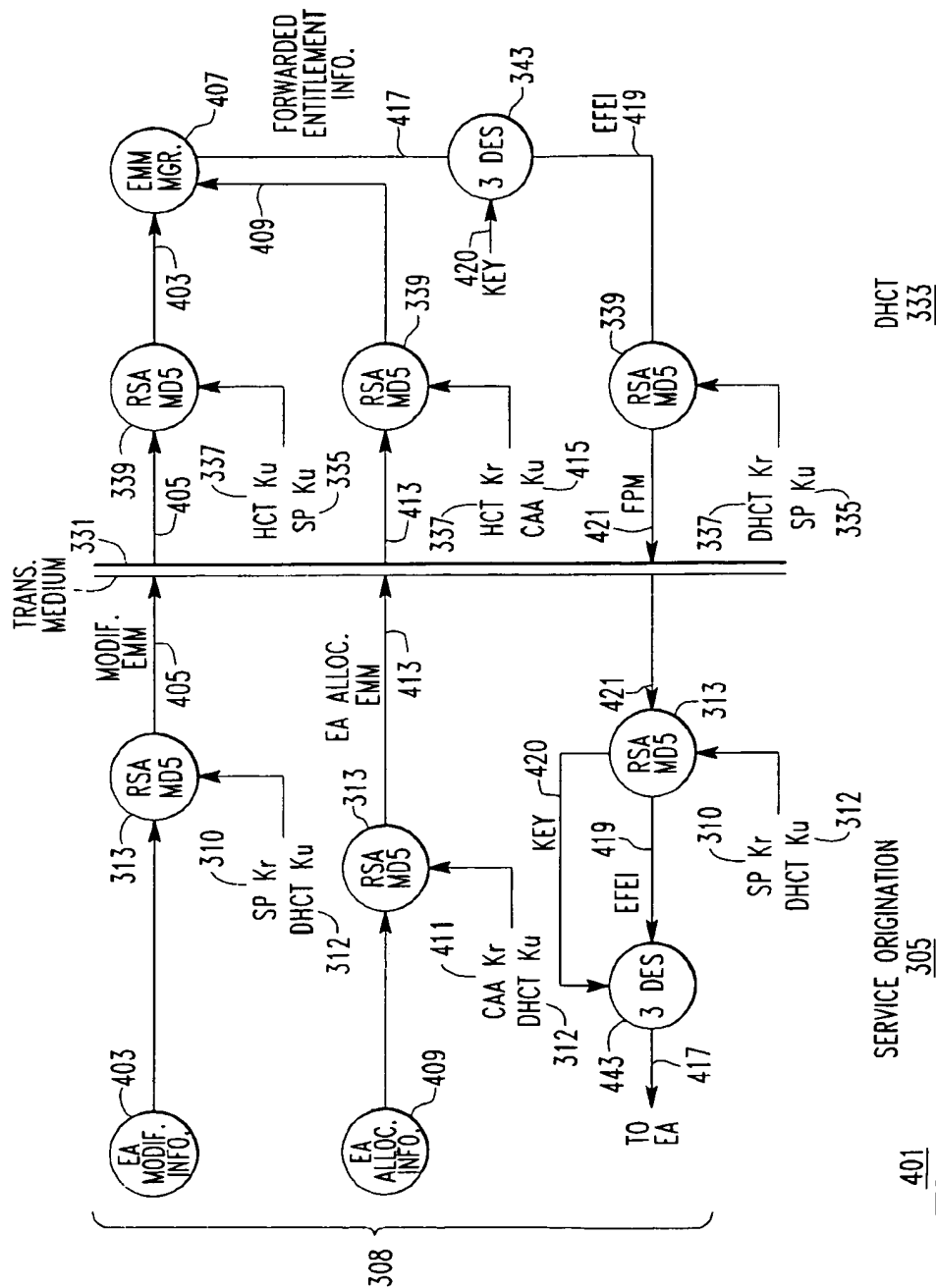


FIG. 3



401
FIG. 4

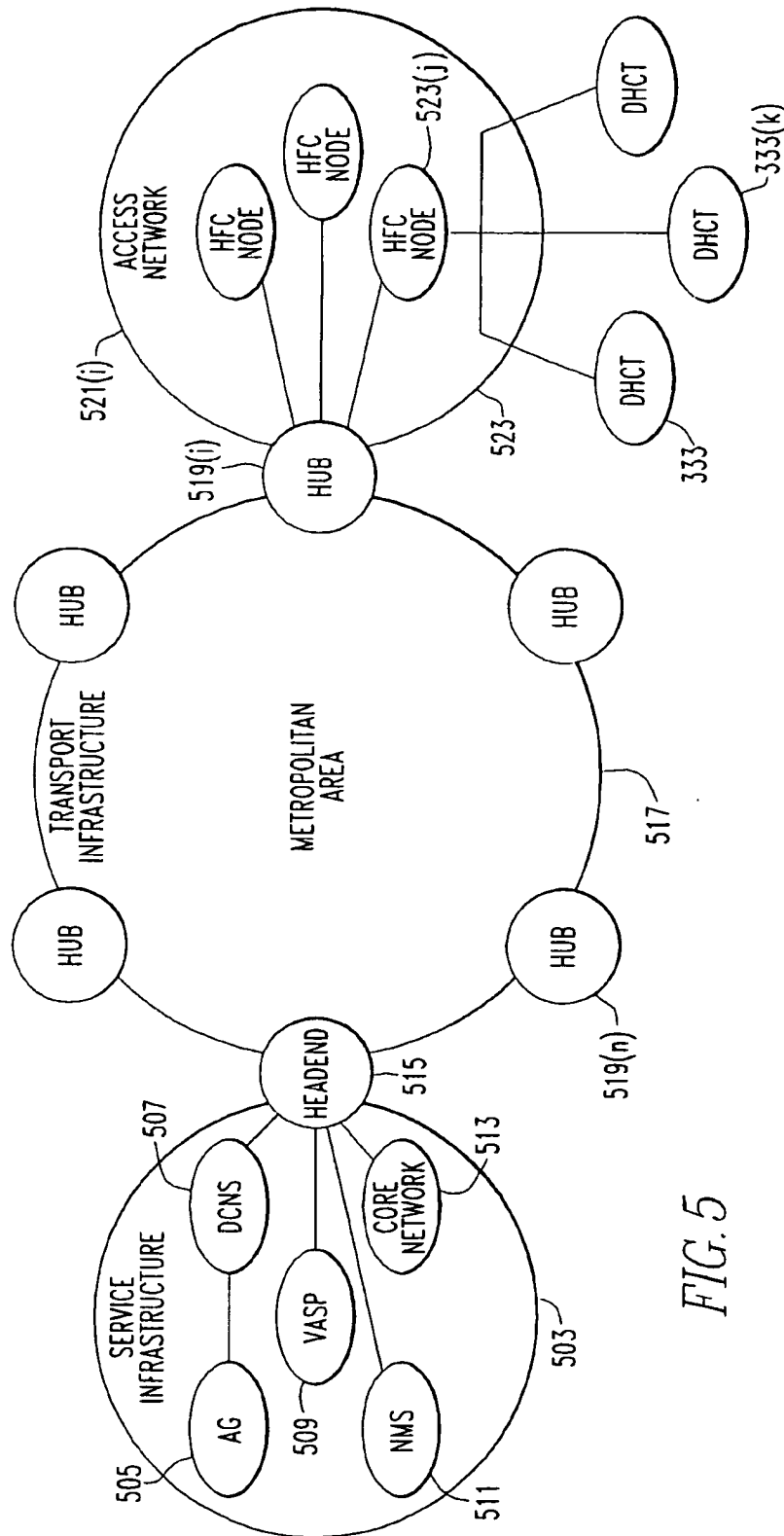
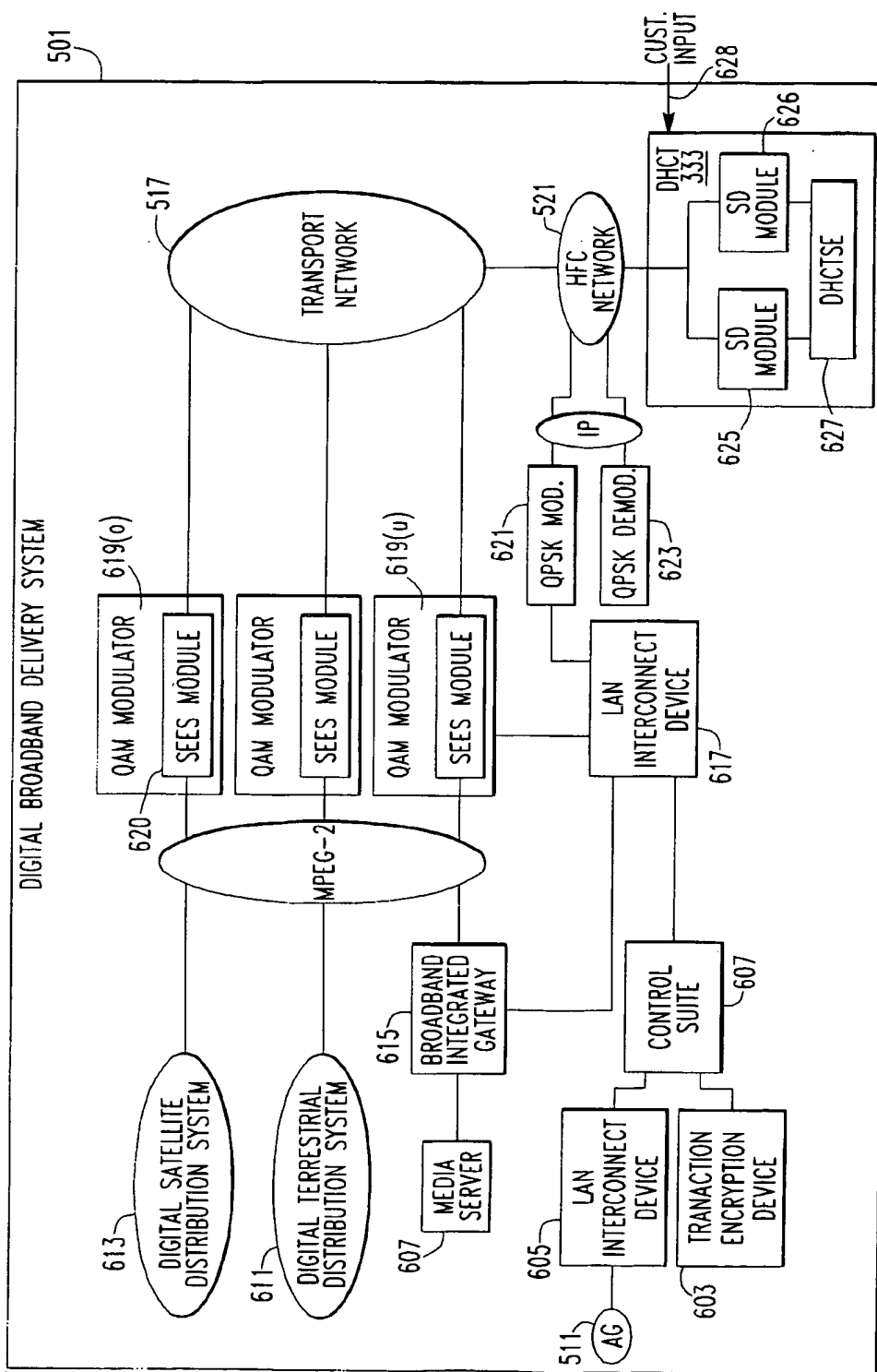
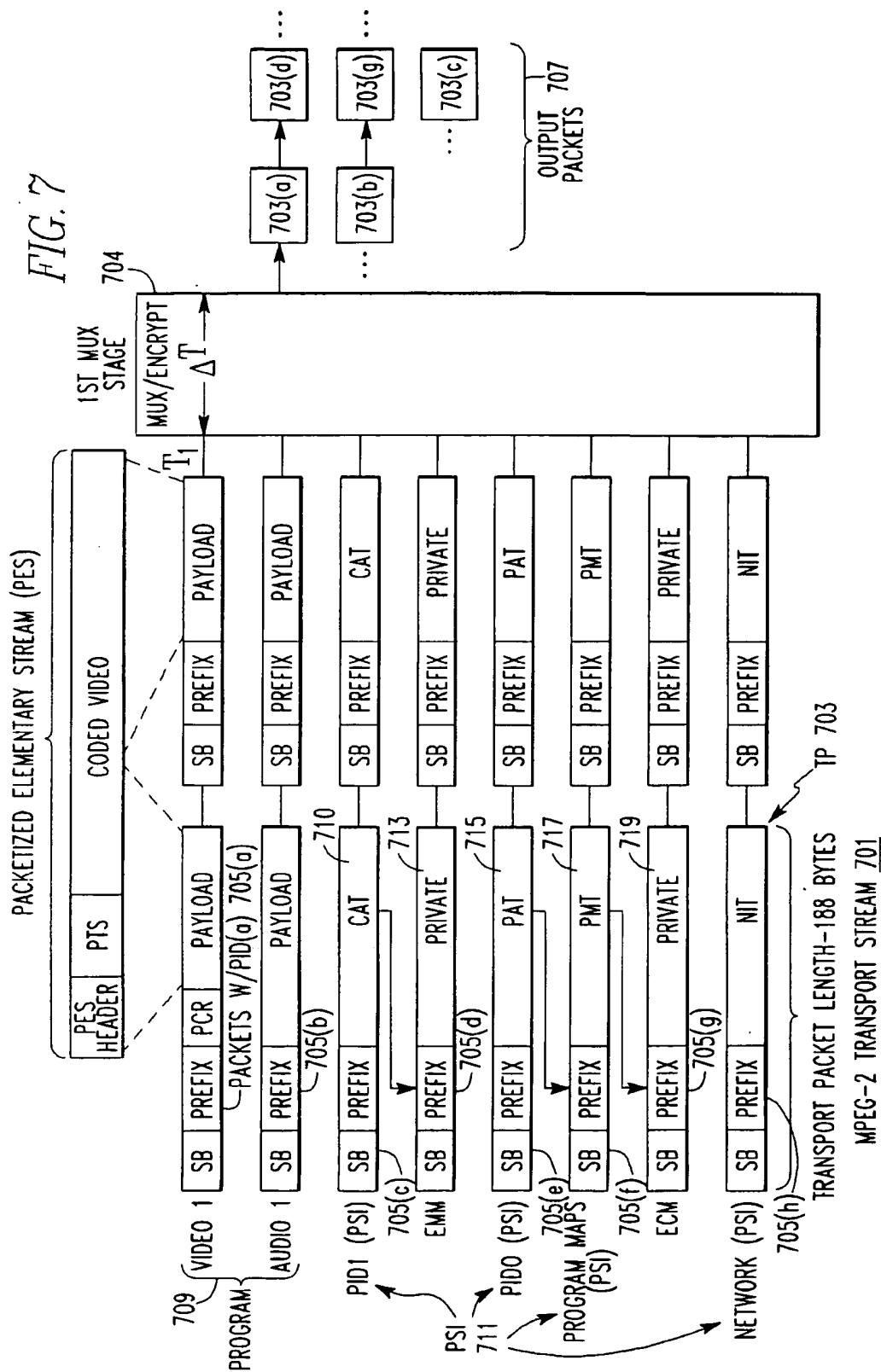


FIG. 5





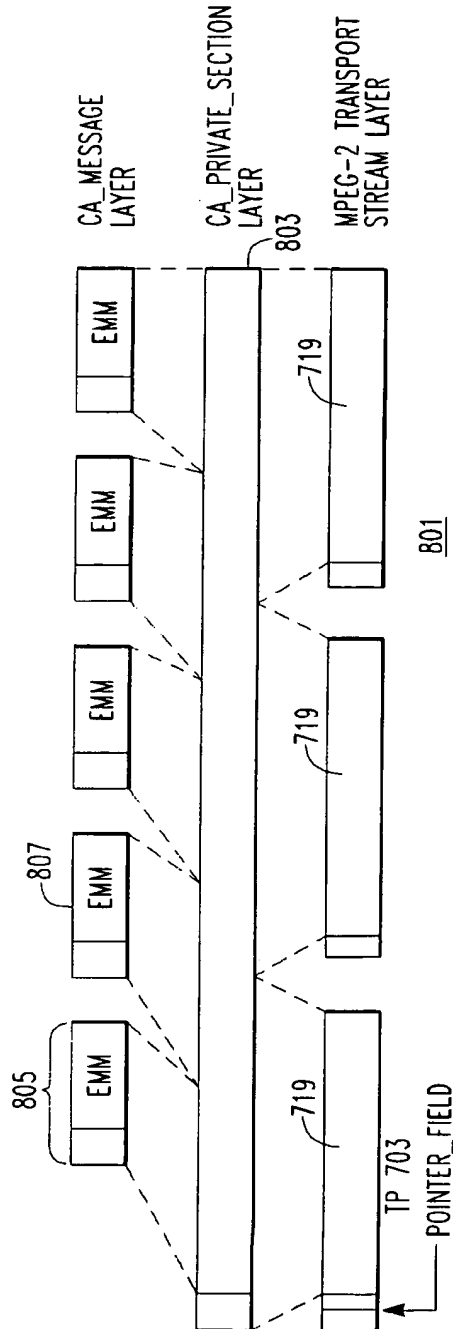


FIG. 8

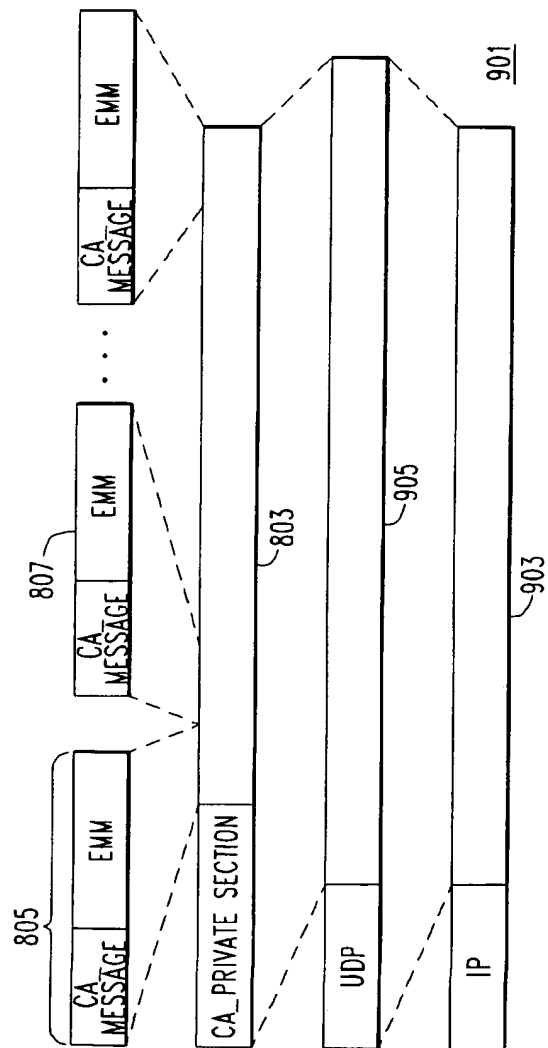


FIG. 9

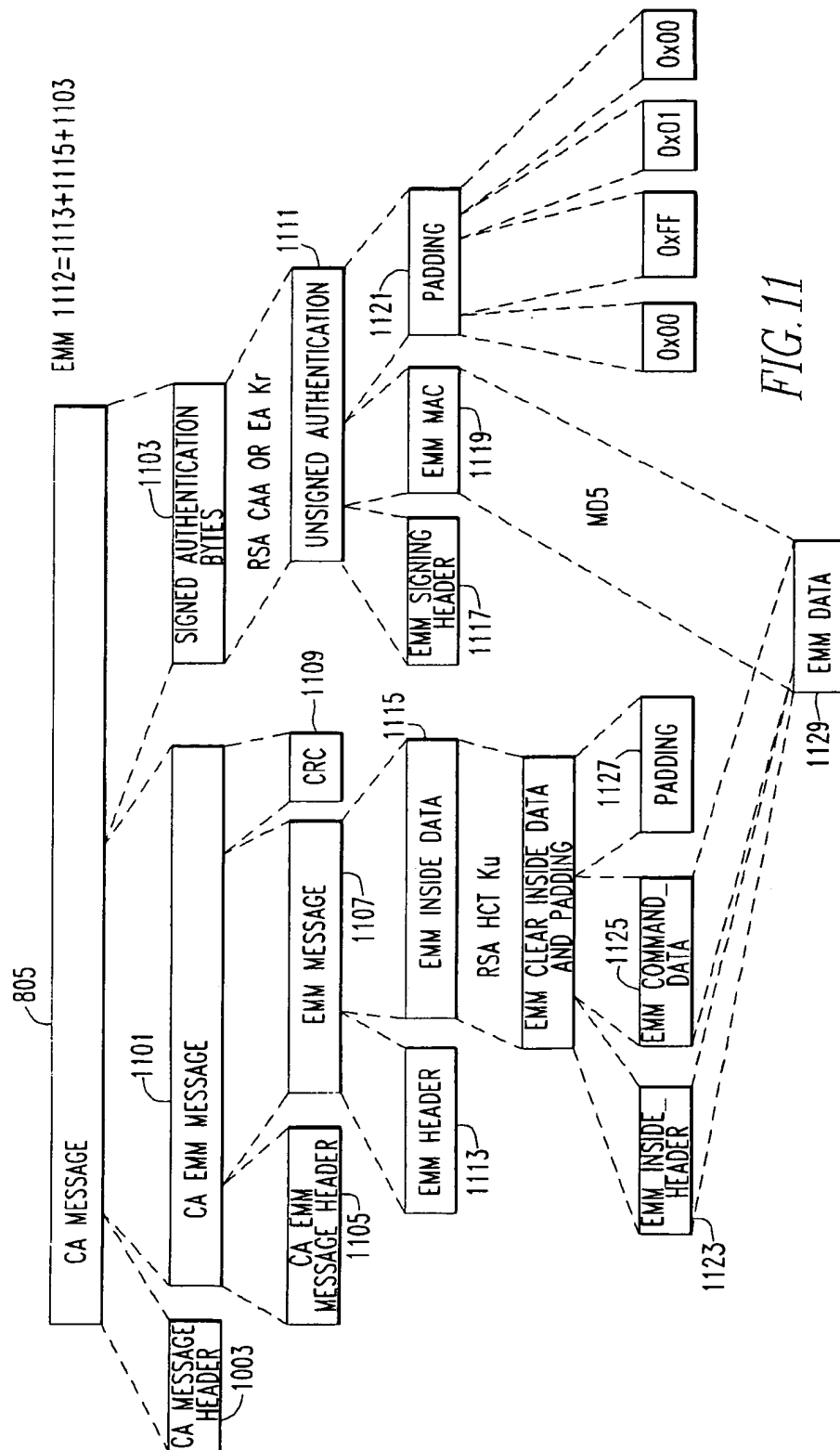
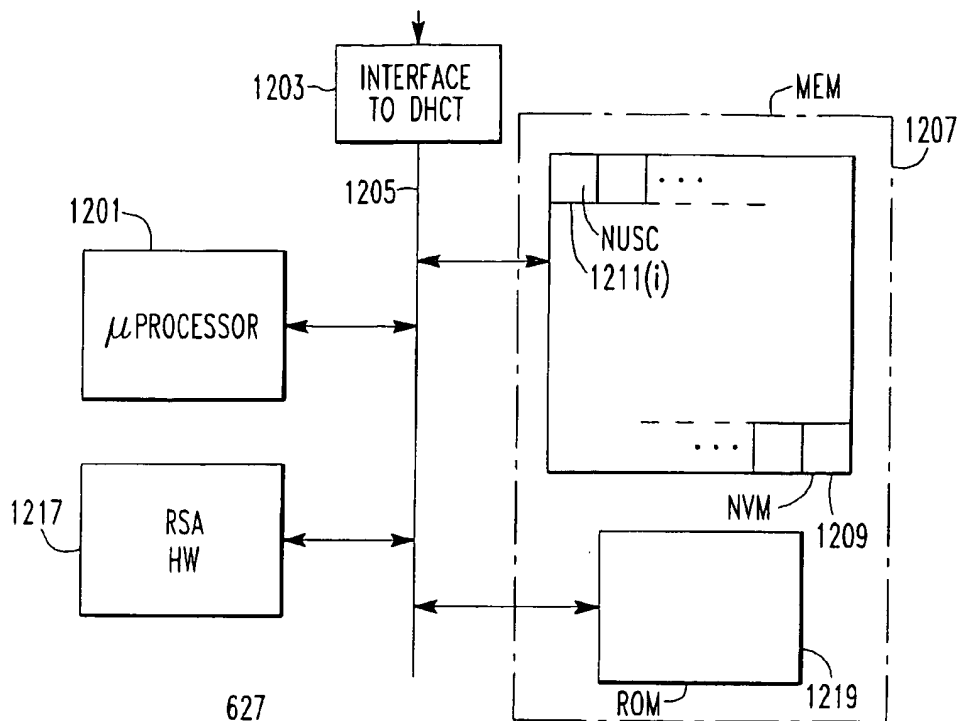
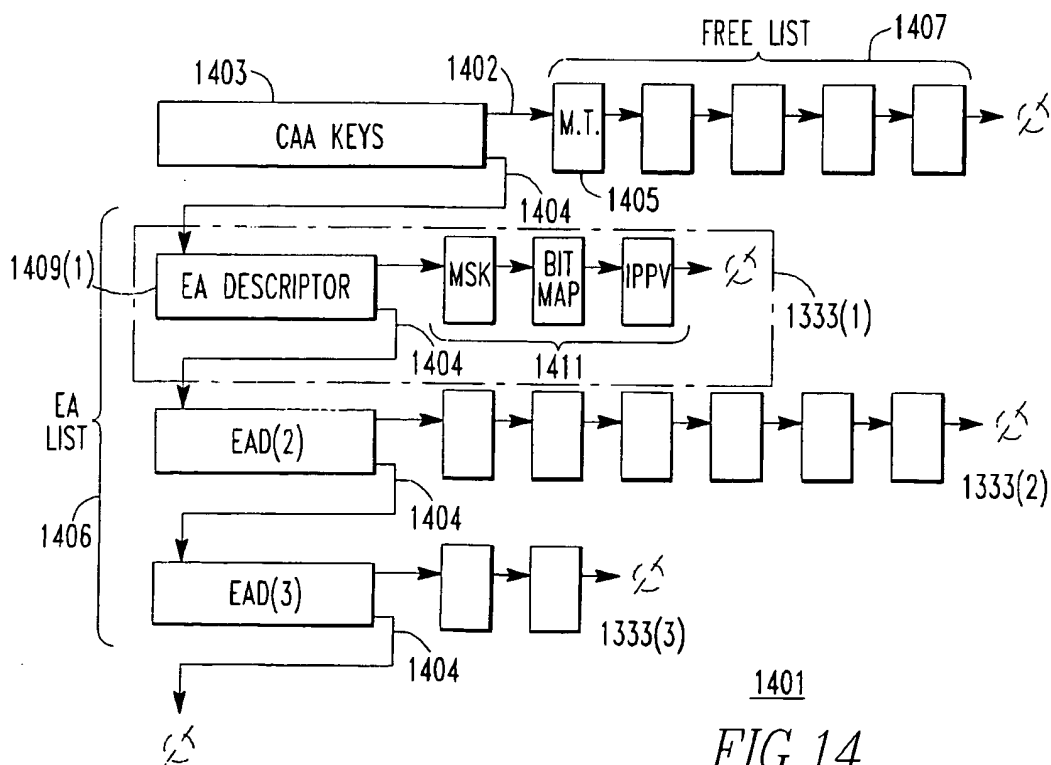


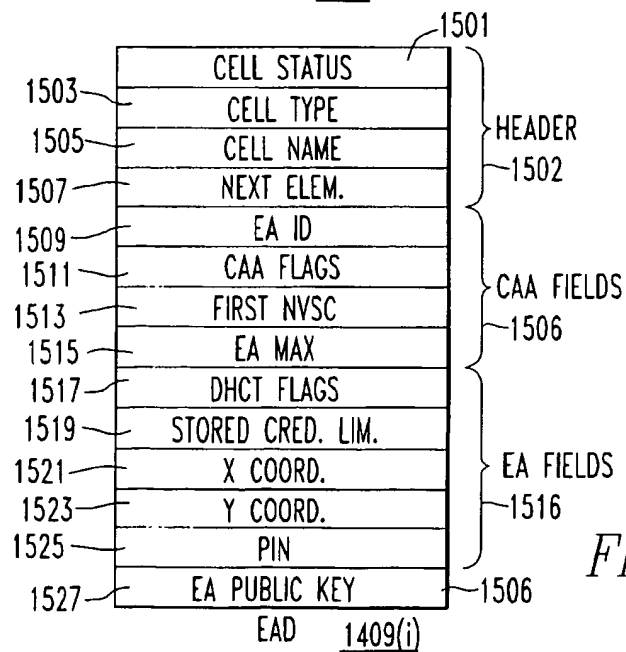
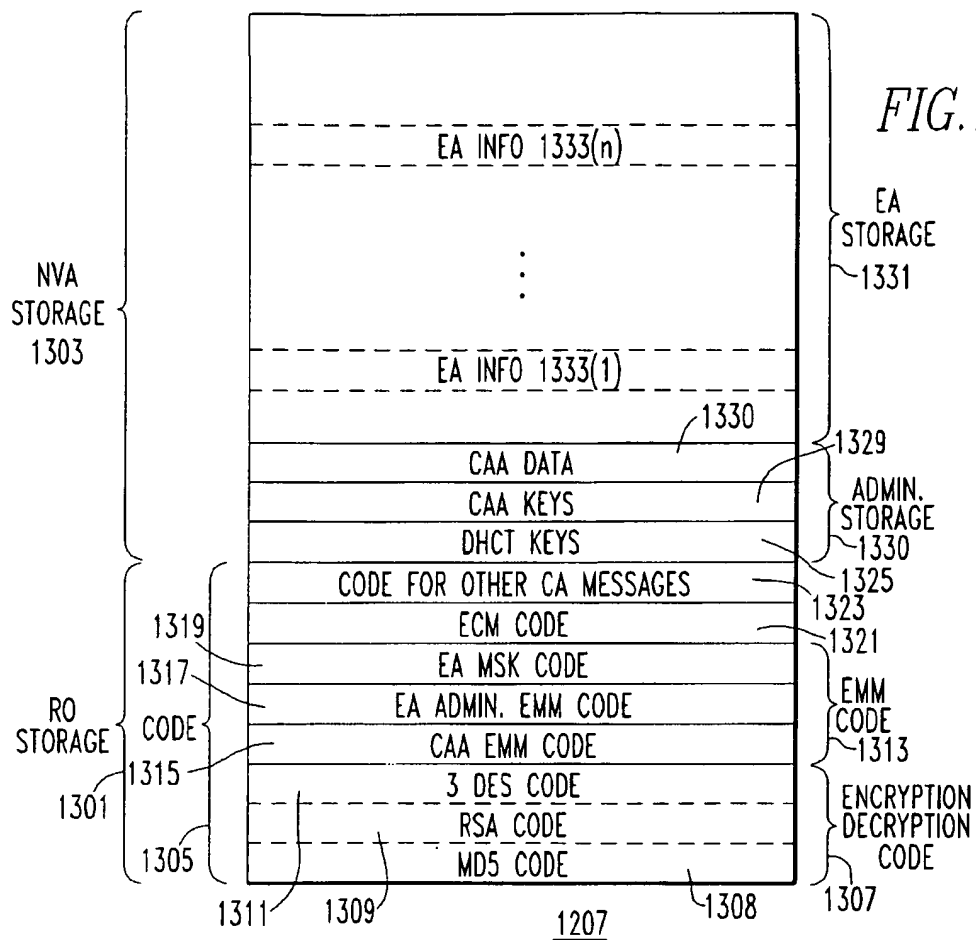
FIG. 11

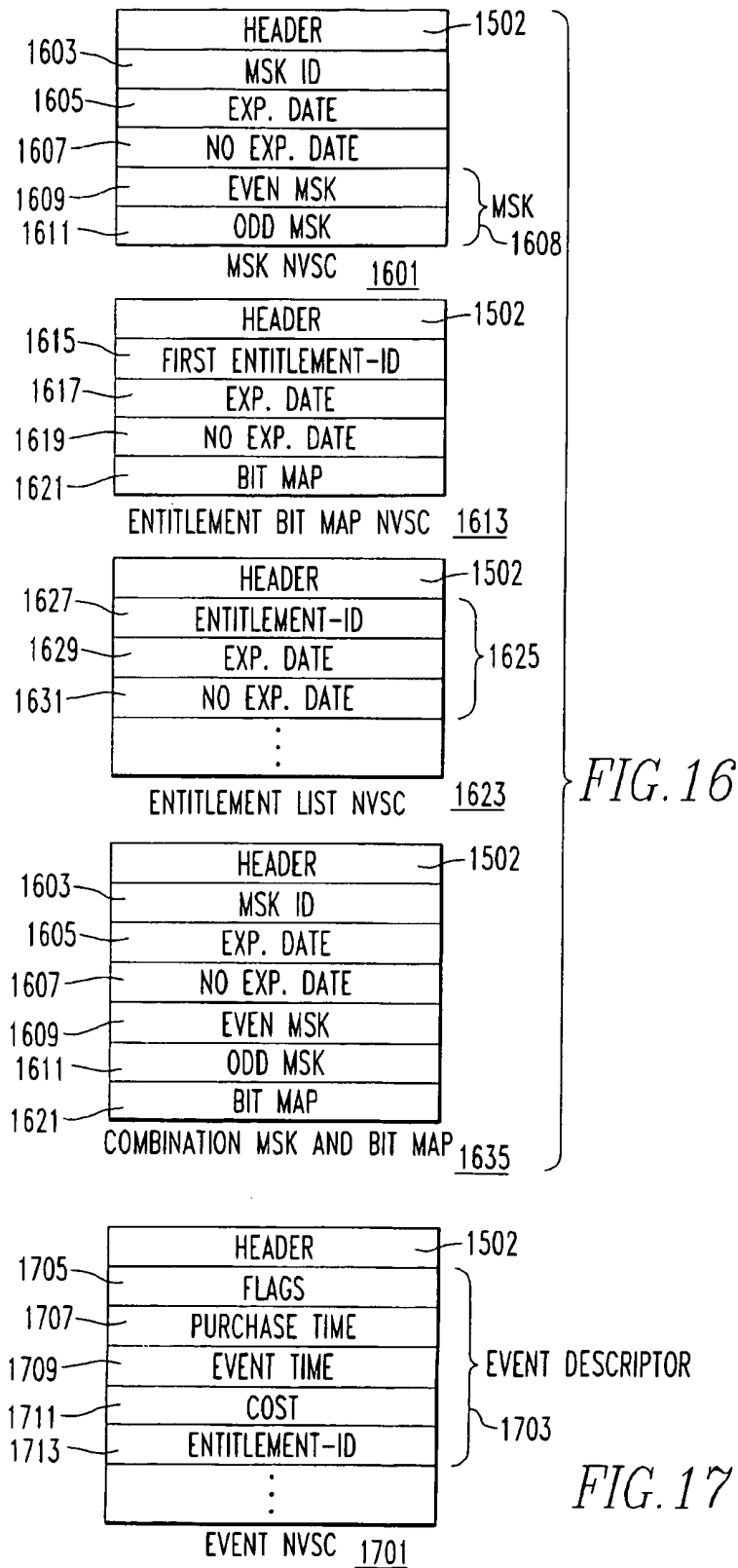


627
FIG. 12



1401
FIG. 14





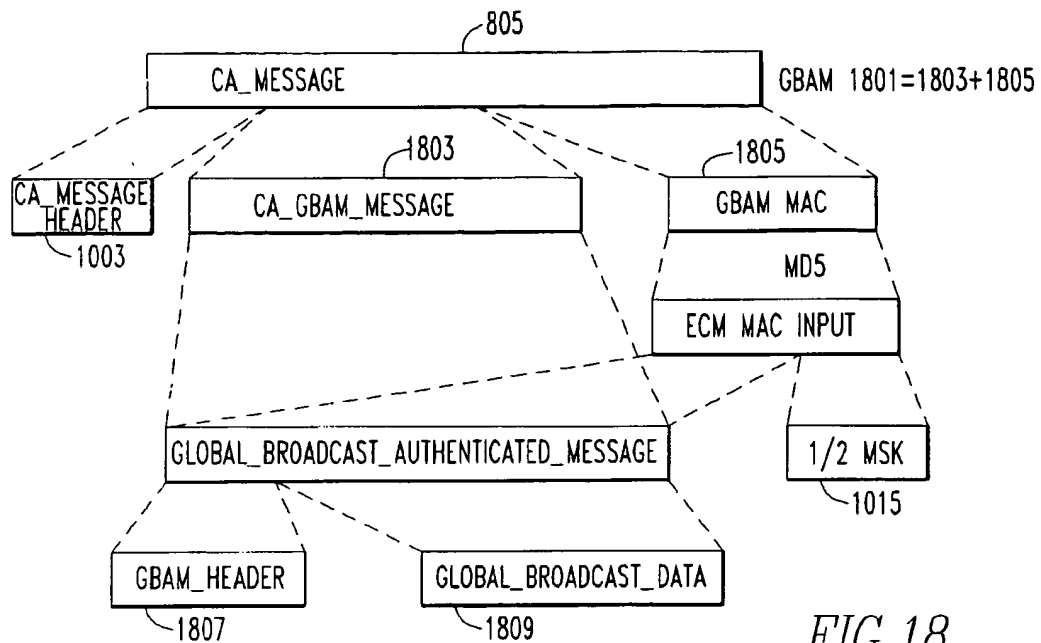


FIG. 18

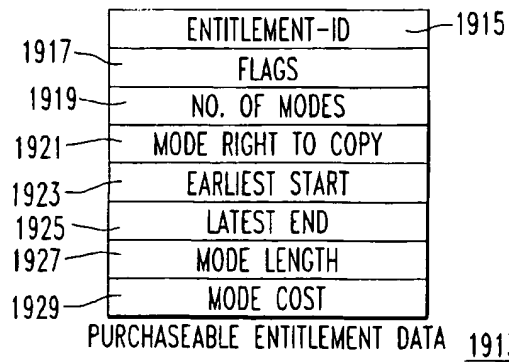
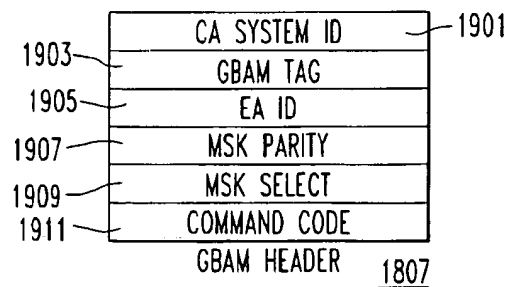


FIG. 19

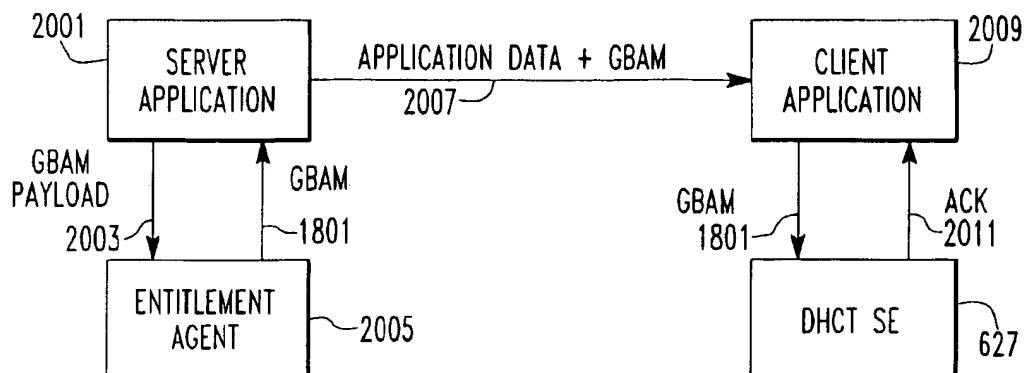


FIG. 20

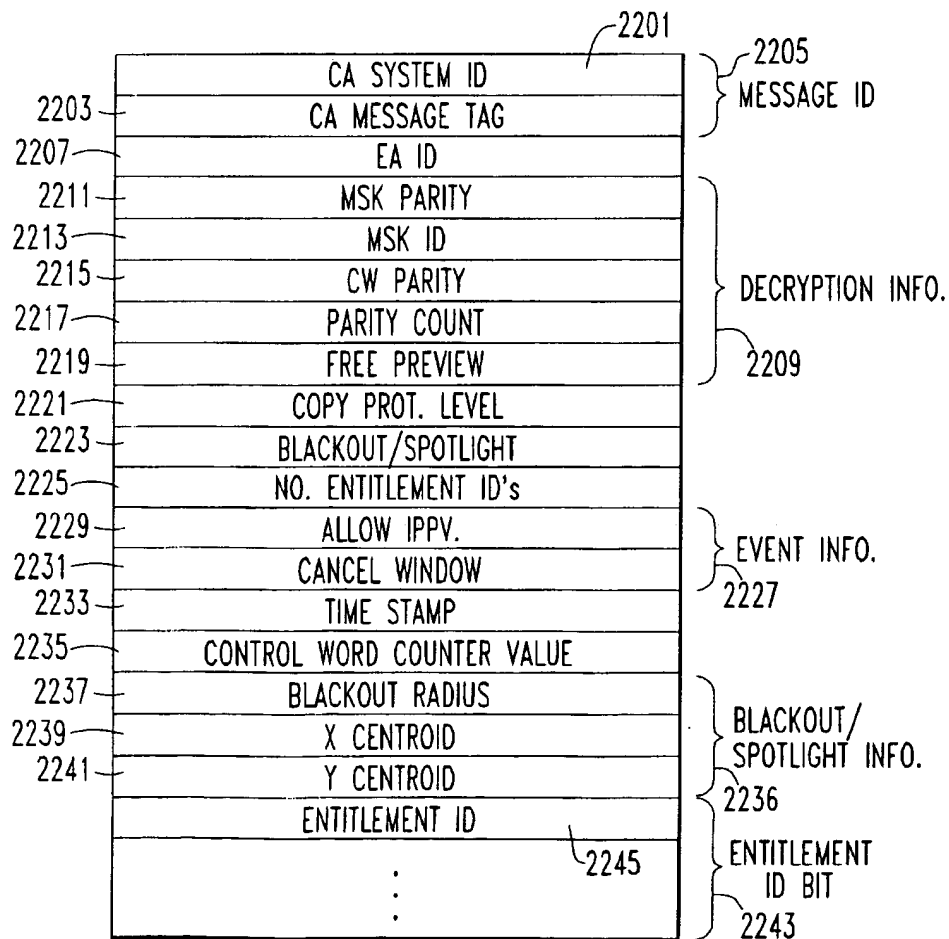


FIG. 22

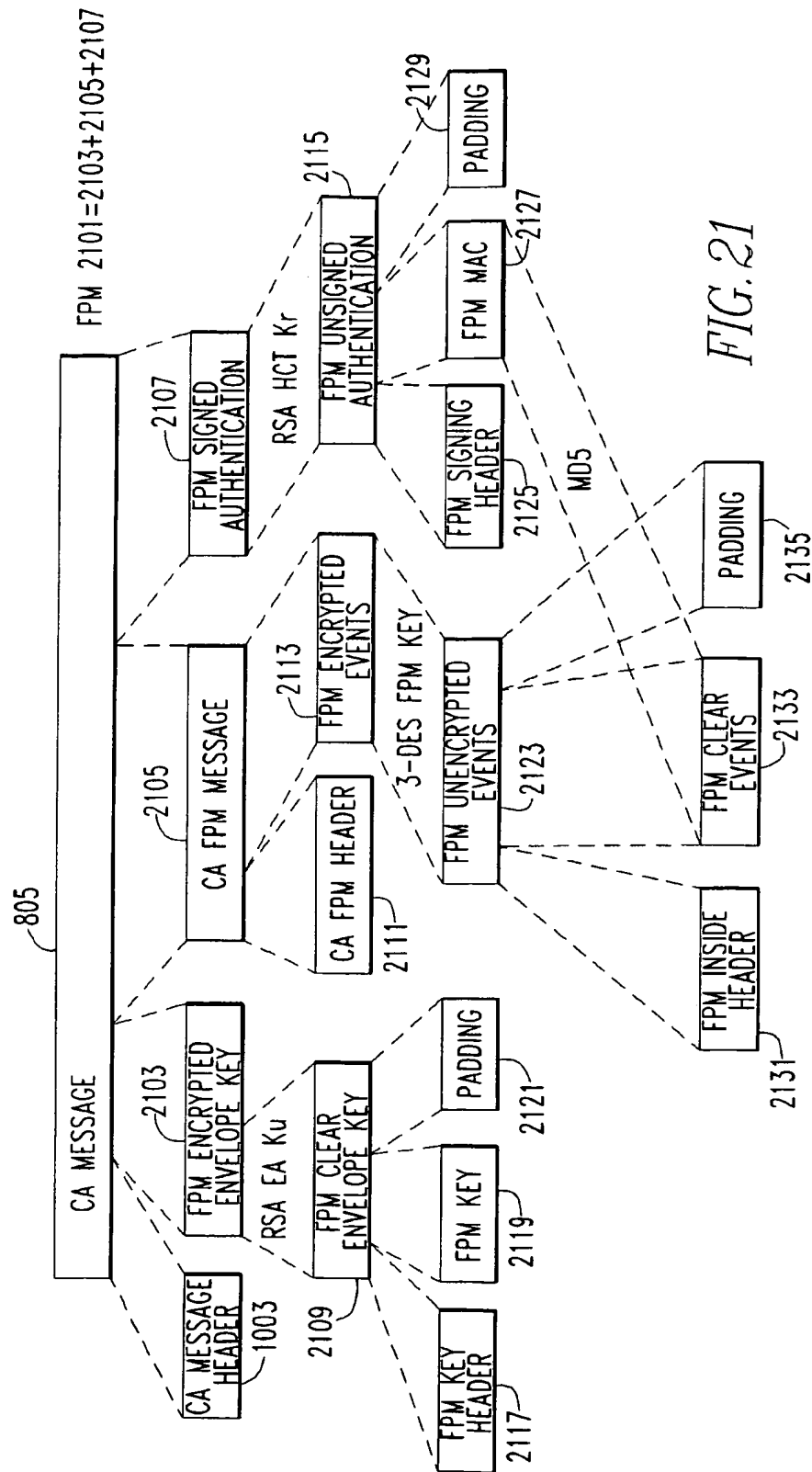


FIG. 21

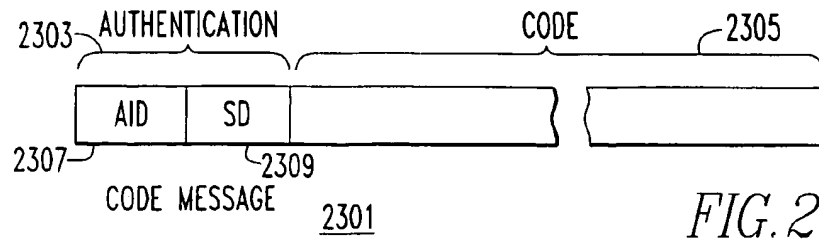


FIG. 23

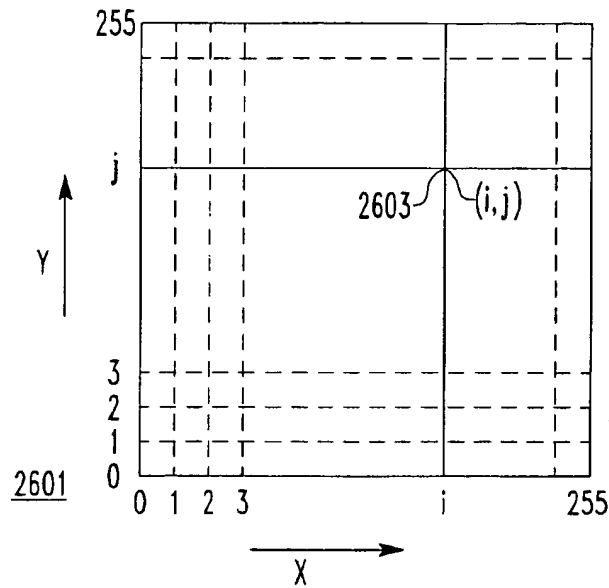


FIG. 26

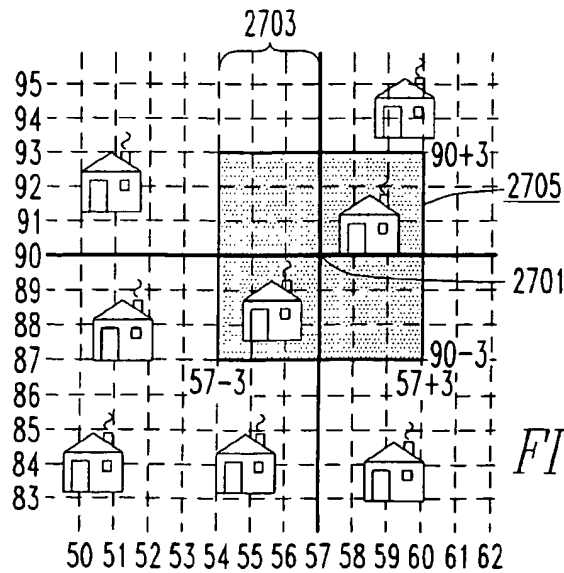
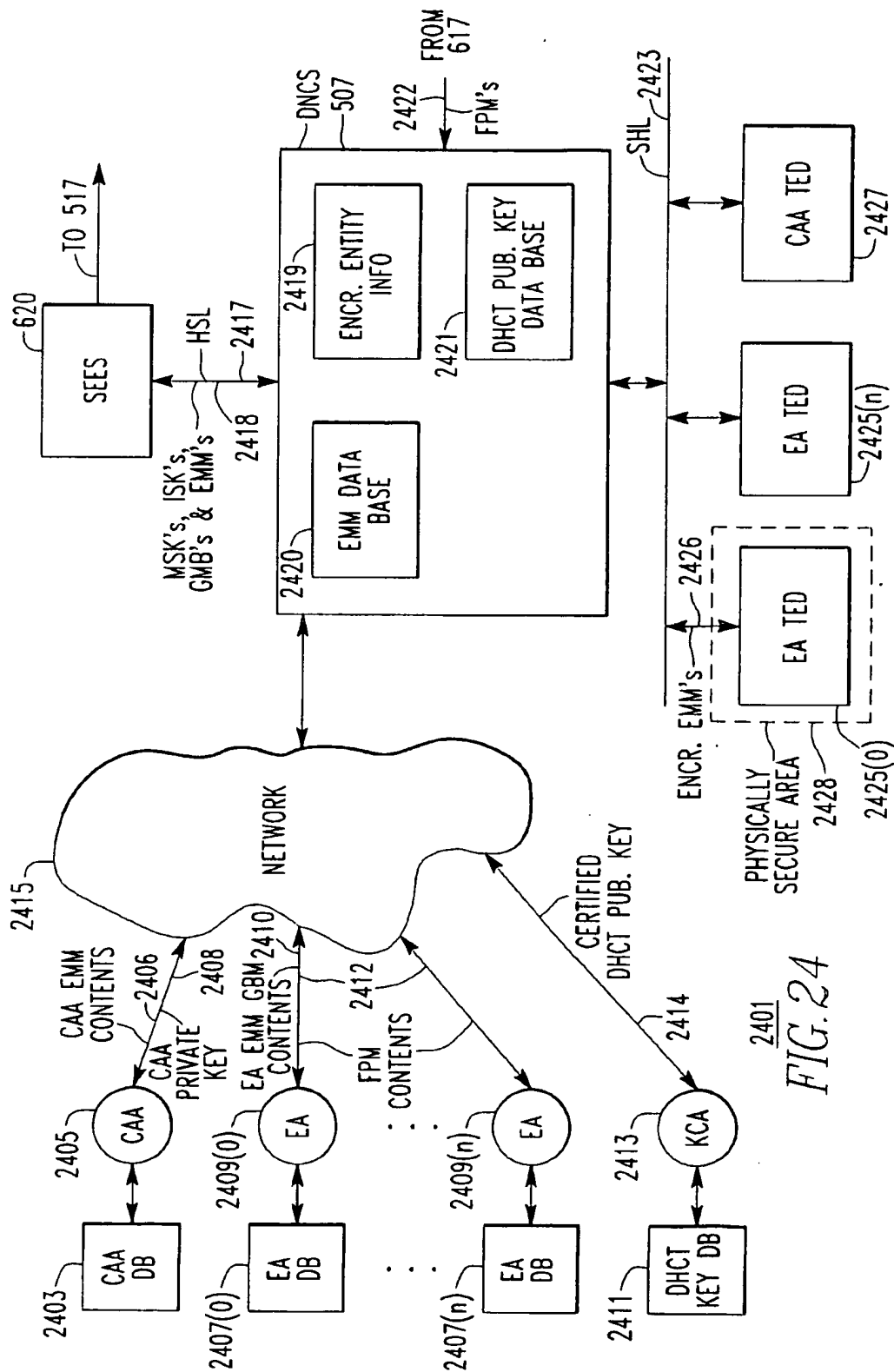


FIG. 27



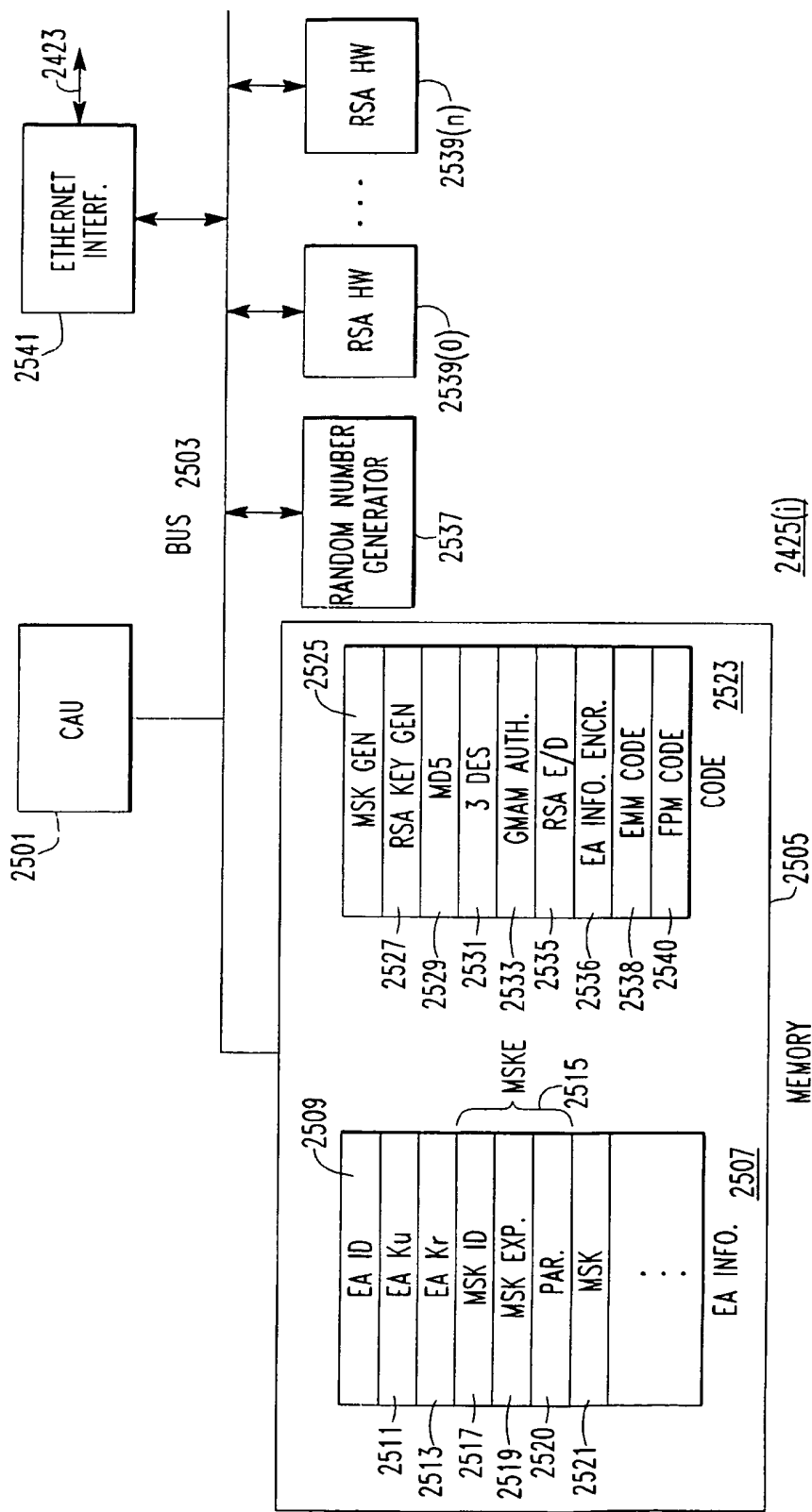


FIG. 25

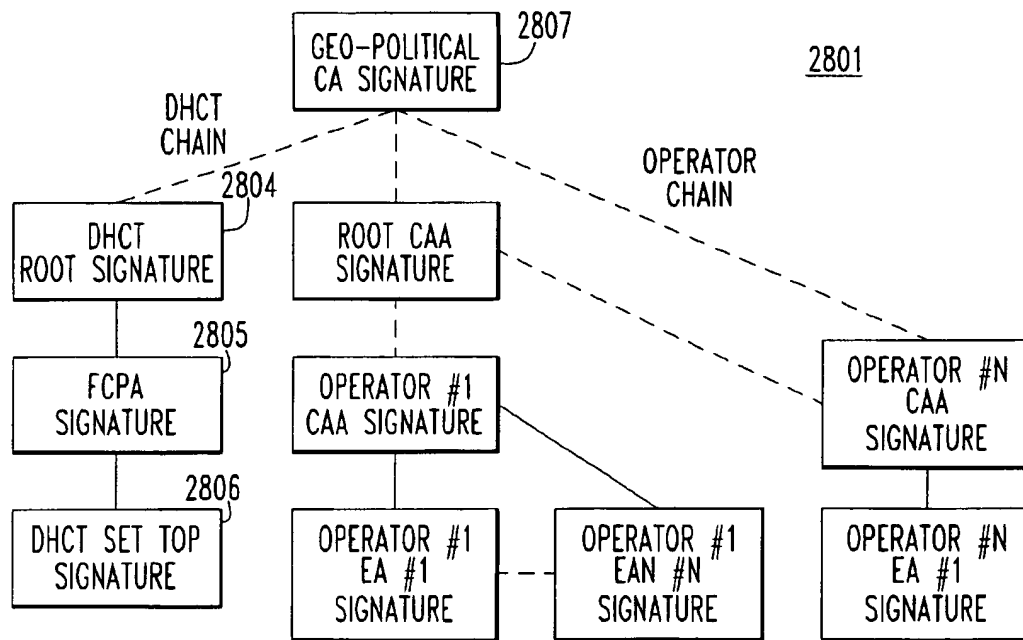


FIG. 28

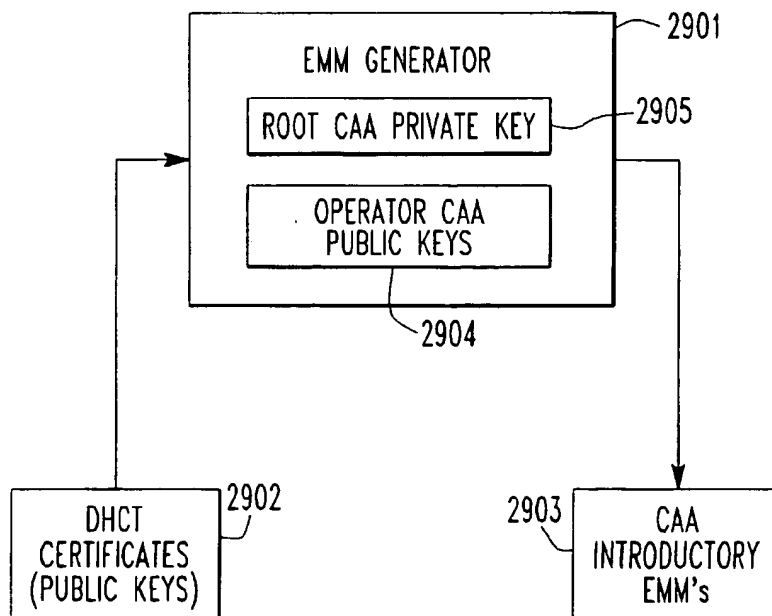


FIG. 29

CONDITIONAL ACCESS SYSTEM**RELATED PATENT APPLICATIONS**

The present patent application is a continuation-in-part of the following U.S. applications, all of which are assigned to the assignee of the present U.S. application:

U.S. Ser. No. 08/767,535, now U.S. Pat. No. 08/6,005, 938, Robert O. Banker and Glendon L. Akins III, Preventing Replay Attacks on Digital information Distributed by Network Service Providers, filed Dec. 16, 1996;

Ser. No. 08/415,617, now U.S. Pat. No. 5,742,677, Pinder, et al., Information Terminal Having Reconfigurable Memory, filed Apr. 3, 1995;

U.S. Ser. No. 08/580,759, now U.S. Pat. No. 5,870,474 Wasilewski, et al., Method and Apparatus for Providing Conditional Access in Connection-Oriented Interactive Networks with a Multiplicity of Service Providers, filed Dec. 29, 1995, which claims the benefit of U.S. Provisional Application No. 60/007,962, filed Dec. 4, 1995;

U.S. Ser. No. 09/111,958, Seaman, et al., Mechanism and Apparatus for Encapsulation of Entitlement Authorization in Conditional Access System, filed Jul. 8, 1998, which claims the benefit of U.S. Provisional Application No. 60/054,578, filed Aug. 1, 1997; abnd

The present patent application also claims priority based on U.S. Ser. No. 60/054,575, Wasilewski et al., Conditional Access System, filed Aug. 1, 1997. The present application is further one of seven applications with identical Detailed Descriptions. All of these applications have the same filing date and all have the same assignee. The titles and inventors of the six applications follow:

(D-3373), Akins, et al., Method and Apparatus for Geographically Limiting Service in a Conditional Access System, filed Jul. 31, 1998;

(D-3457), Wasilewski, et al., Authorization of Services in a Conditional Access System, filed Jul. 31, 1998;

(D-3472), Akins, et al., Representing Entitlements to Service in a Conditional Access System, filed Jul. 31, 1998;

(D-3365), Pinder, et al., Encryption Devices for use in a Conditional Access System, filed Jul. 31, 1998;

(D-2999), Pinder, et al., Verification of the Source of Program Information in a Conditional Access System, filed Jul. 31, 1998;

(D-3614), Pinder, et al., Source Authentication of Download Information in a Conditional Access System, filed Jul. 31, 1998.

FIELD OF THE INVENTION

The invention concerns systems for protecting information and more particularly concerns systems for protecting information that is transmitted by means of a wired or wireless medium against unauthorized access.

BACKGROUND OF THE INVENTION

One way of distributing information is to broadcast it, that is, to place the information on a medium from which it can be received by any device that is connected to the medium. Television and radio are well-known broadcast media. If one wishes to make money by distributing information on a broadcast medium, there are a couple of alternatives. A first is to find sponsors to pay for broadcasting the information. A second is to permit access to the broadcast information only to those who have paid for it. This is generally done by broadcasting the information in scrambled or encrypted

form. Although any device that is connected to the medium can receive the scrambled or encrypted information, only the devices of those users who have paid to have access to the information are able to unscramble or decrypt the information.

A service distribution organization, for example a CATV company or a satellite television company, provides its subscribers with information from a number of program sources, that is, collections of certain kinds of information. For example, the History Channel is a program source that provides television programs about history. Each program provided by the History Channel is an "instance" of that program source. When the service distribution organization broadcasts an instance of the program source, it encrypts or scrambles the instance to form encrypted instance. An encrypted instance contains instance data, which is the encrypted information making up the program.

An encrypted instance is broadcast over a transmission medium. The transmission medium may be wireless or it may be "wired", that is, provided via a wire, a coaxial cable, or a fiber optic cable. It is received in a large number of set top boxes. The function of set-top box is to determine whether encrypted instance should be decrypted and, if so, to decrypt it to produce a decrypted instance comprising the information making up the program. This information is delivered to a television set. Known set top boxes include decryptors to decrypt the encrypted instance.

Subscribers generally purchase services by the month (though a service may be a one-time event), and after a subscriber has purchased a service, the service distribution organization sends the set top box belonging to the subscriber messages required to provide the authorization information for the purchased services. Authorization information may be sent with the instance data or may be sent via a separate channel, for example, via an out-of-band RF link, to a set top box. Various techniques have been employed to encrypt the authorization information. Authorization information may include a key for a service of the service distribution organization and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information indicates that the subscriber is entitled to watch the program of an encrypted instance, the set-top box decrypts the encrypted instance.

It will be appreciated that "encryption" and "scrambling" are similar processes and that "decryption" and "descrambling" are similar processes; a difference is that scrambling and descrambling are generally analog in nature, while encryption and decryption processes are usually digital.

The access restrictions are required in both analog and digital systems. In all systems, the continued technological improvements being used to overcome the access restrictions require more secure and flexible access restrictions. As more systems switch from an analog format to a digital format, or a hybrid system containing both analog and digital formats, flexible access restrictions will be required.

Restricting access to broadcast information is even more important for digital information. One reason for this is that each copy of digital information is as good as the original; another is that digital information can be compressed, and consequently, a given amount of bandwidth carries much more information in digital form; a third is that the service distribution organizations are adding reverse paths which permit a set-top box to send a message to the service distribution organization, thereby permitting various interactive services.

Thus, the service distribution organizations require access restrictions which are both more secure and more flexible than those in conventional systems

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a conditional access system;
FIG. 2A is a block diagram of the service instance encryption techniques disclosed herein;

FIG. 2B is a block diagram of the service instance decryption techniques disclosed herein;

FIG. 3 is a more detailed block diagram of the service instance encryption and decryption techniques disclosed herein;

FIG. 4 is a block diagram of the techniques used to dynamically provide entitlement agents to a DHCT;

FIG. 5 is a block diagram of a digital broadband delivery system in which the conditional access system is implemented;

FIG. 6 is a block diagram of the conditional access system in the digital broadband delivery system of FIG. 5;

FIG. 7 is a diagram of an MPEG-2 transport stream;

FIG. 8 is a diagram of how EMMs are mapped into an MPEG-2 transport stream;

FIG. 9 is a diagram of how EMMs are mapped into an IP packet;

FIG. 10 is a diagram of how ECMs are mapped into a MPEG-2 transport stream;

FIG. 11 is a detailed diagram of an EMM.

FIG. 12 is a detailed diagram of a preferred embodiment of DHCTSE 627;

FIG. 13 is a diagram of the contents of memory in DHCTSE 627;

FIG. 14 is a diagram of how NVSCs are allocated to entitlement agents in a preferred embodiment;

FIG. 15 is a diagram of an EAD NVSC;

FIG. 16 is a diagram of other kinds of NVSCs;

FIG. 17 is a diagram of an event NVSC;

FIG. 18 is a diagram of a global broadcast authenticated message (GBAM);

FIG. 19 is a detail of the contents of one kind of GBAM;

FIG. 20 is a diagram showing how GBAMs may be used generally to provide data to a client application;

FIG. 21 is a diagram of a forwarded purchase message;

FIG. 22 is a diagram of the entitlement unit message in an ECM;

FIG. 23 is a diagram of a code message;

FIG. 24 is a diagram showing the relationship between TEDs and the rest of conditional access system 601;

FIG. 25 is a detailed diagram of a TED;

FIG. 26 is an illustration of the coordinate system used for spotlight and blackout;

FIG. 27 shows how an area is computed in the coordinate system of FIG. 26;

FIG. 28 is a description of a public key hierarchy; and

FIG. 29 is a description of an EMM generator according to the present invention.

The reference numbers in the drawings have at least three digits. The two rightmost digits are reference numbers within a figure; the digits to the left of those digits are the number of the figure in which the item identified by the reference number first appears. For example, an item with reference number 203 first appears in FIG. 2.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

The following Detailed Description will first provide a general introduction to a conditional access system and to

encryption and decryption, will then describe how service instance encoding and decoding is done in a preferred embodiment, and will thereupon describe the techniques used in the preferred embodiment to authenticate the ECMs and EMMs of the preferred embodiment. Next, the Detailed Description will describe how EMMs can be used to dynamically add and remove access to services and the role of encryption and authentication in these operations. Finally, there will be a detailed exposition of how the techniques described in the foregoing are employed in a broadcast data delivery system with a node structure and a reverse path from the set top box to the head end, of how secure processors and memory are employed in the preferred embodiment to protect keys and entitlement information, and of how certain operations are performed in the preferred embodiment.

Conditional Access System Overview

FIG. 1 provides an overview of a system 101 for limiting access to broadcast information. Such systems will be termed in the as "conditional access systems". A service distribution organization 103, for example a CATV company or a satellite television company, provides its subscribers with information from a number of services, that is, collections of certain kinds of information. For example, the History Channel is a service that provides television programs about history. Each program provided by the History Channel is an "instance" of that service. When the service distribution organization broadcasts an instance of the service, it encrypts or scrambles the instance to form encrypted instance 105. Encrypted instance 105 contains instance data 109, which is the encrypted information making up the program, and entitlement control messages (ECM) 107. The entitlement control messages contain information needed to decrypt the encrypted portion of the associated instance data 109. A given entitlement control message is sent many times per second, so that it is immediately available to any new viewer or a service. In order to make decryption of instance data 109 even more difficult for pirates, the content of the entitlement control message is changed every few seconds, or more frequently.

Encrypted instance 105 is broadcast over a transmission medium 112. The medium may be wireless or it may be "wired", that is, provided via a wire, a coaxial cable, or a fiber optic cable. It is received in a large number of set top boxes 113(0 . . . n), each of which is attached to a television set. It is a function of set-top box 113 to determine whether encrypted instance 105 should be decrypted and if so, to decrypt it to produce decrypted instance 123, which is delivered to the television set. As shown in detail with regard to set top box 113(0), set top box 113 includes decryptor 115, which uses a control word 117 as a key to decrypt encrypted instance 105. Control word 117 is produced by control word generator 119 from information contained in entitlement control message 107 and information from authorization information 121 stored in set-top box 113. For example, authorization information 121 may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information 121 indicates that the subscriber is entitled to watch the program of encrypted instance 105, control word generator 119 uses the key together with information from ECM 107 to generate control word 117. Of course, a new control word is generated for each new ECM 107.

The authorization information used in a particular set top box 113(i) is obtained from one or more entitlement management messages 111 addressed to set top box 113(i). Subscribers generally purchase services by the month

(though a service may be a one-time event), and after a subscriber has purchased a service, service distribution organization 103 sends set top box 113(i) belonging to the subscriber entitlement management messages 111 as required to provide the authorization information 121 required for the purchased services. Entitlement management messages (EMMs) may be sent interleaved with instance data 109 in the same fashion as ECMs 107, or they may be sent via a separate channel, for example via an out-of-band RF link, to set top box 113(i), which stores the information from the entitlement management message (EMM) 111 in authorization information 121. Of course, various techniques have been employed to encrypt entitlement management messages 111.

Encryption and Decryption Generally

The encryption and decryption techniques used for service instance encoding and decoding belong to two general classes: symmetrical key techniques and public key techniques. A symmetrical key encryption system is one in which each of the entities wishing to communicate has a copy of a key; the sending entity encrypts the message using its copy of the key and the receiving entity decrypts the message using its copy of the key. An example symmetrical key encryption-decryption system is the Digital Encryption Standard (DES) system. A public key encryption system is one in which each of the entities wishing to communicate has its own public key-private key pair. A message encrypted with the public key can only be decrypted with the private key and vice-versa. Thus, as long as a given entity keeps its private key secret, it can provide its public key to any other entity that wishes to communicate with it. The other entity simply encrypts the message it wishes to send to the given entity with the given entity's public key and the given entity uses its private key to decrypt the message. Where entities are exchanging messages using public key encryption, each entity must have the other's public key. The private key can also be used in digital signature operations, to provide authentication. For details on encryption generally and symmetrical key and public key encryption in particular, see Bruce Schneier, *Applied Cryptography*, John Wiley and Sons, New York, 1994.

The design of an encryption system for a given application involves a number of considerations. As will be seen in the following, considerations that are particularly important in the broadcast message environment include the following:

key security: A symmetrical key system is useless if a third party has access to the key shared by the communicating parties, and a public key system is also useless if someone other than the owner of a given public key has access to the corresponding private key.

key certification: how can the recipient of a key be sure that the key he or she has received is really a key belonging to the entity to which the recipient wishes to send an encrypted message and not a key belonging to another entity which wishes to intercept the message?

message authentication: how can the recipient of a message be sure that the message is from the party it claims to be from, and/or that the message has not been altered?

speed of encryption and decryption: in general, symmetrical key encryption systems are faster than public key encryption systems and are preferred for use with real-time data.

key size: in general, the longer the key used in an encryption system, the more resources will be required to break the encryption and thereby gain access to the message.

All of the foregoing considerations are influenced by the fact that the environment in which a conditional access system operates must be presumed to be hostile. Many customers of broadcast services see nothing wrong with cheating the service provider and have nothing against tampering physically with the portion of the conditional access system that is contained in the receiver or using various cryptographic attacks to steal keys or to deceive the receiver about the source of the messages it receives. Moreover, the providers of the systems that actually broadcast the services do not necessarily have the same interests as the providers of the service content, and therefore need to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver.

Service Instance Encryption and Decryption: FIGS. 2A and 2B

In overview, the encryption system of the present invention uses symmetrical key encryption techniques to encrypt and decrypt the service instance and public key encryption techniques to transport a copy of one of the keys used in the symmetrical key techniques of the key from the service provider to the set-top box.

In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be combined with other elementary streams and private data, such as conditional access data. The key used in the Program Encrypt function 201 is called the Control Word (CW) 202. The CW 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs. A new CW is generated frequently, perhaps once every few seconds and is applied to each elementary stream on the same time scale. Each new CW is encrypted by Control Word Encrypt & Message Authenticate function 204 using a Multi-Session key (MSK) 208 provided by Multi-Session Key generator 205. The CW is then combined into an ECM 107 with other service-related information. The ECM 107 is authenticated by Control Word Encrypt & Message Authenticate function 204 which produces a message authentication code using a keyed-hash value derived from the message content combined with a secret which can be shared with the receiving set-top box 113. This secret is preferably part or all of the MSK 208. The message authentication code is appended to the rest of the ECM 107. The CW 202 is always encrypted before being sent along with the other parts of the ECM to MUX 200. This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208).

The MSK 208 has a longer lifetime than CW 202. The MSK lifetime is typically hours to days in length. MSK 208 is both encrypted and digitally signed by MSK Encrypt & Digital Signature function 206 before being sent to MUX 200 encapsulated in EMM 111. MSK 208 and other parts of EMM 111 are preferably encrypted using a public key algorithm, such as the well-known RSA algorithm, with a public key associated with the specific set-top box 113 to which the EMM is addressed. The public keys of all set-top boxes 113 in a system 101 are stored in Public Key Data Base 207. The public keys in this data base are preferably certified by a certificate authority. The digital signature

7

function in 206 is preferably the RSA digital signature method, although others could be used. In the case of an RSA digital signature, the private key which is used to make the signature belongs to the entitlement agent within service distribution organization 103 responsible for authorizing the associated service.

In FIG. 2B, the corresponding DHCT private key and associated DHCT public secure micro serial number are stored in memory 232 of decoder 240. Public secure micro serial number is provided so that demultiplexer 230 can select an encrypted multi-session key addressed to decoder 240 from transport data stream (TDS). Encrypted multi-session key $E_{K_{pr}}$ (MSK) is decrypted in decryptor 234 using DHCT private key from memory 232 to provide multi-session key MSK. Demultiplexer 230 also selects from transport data stream TDS encrypted control word (CW) E_{MSK} (CW). The encrypted CW is processed in decryptor 236 using multi-session key MSK as the decryption key to provide the unencrypted CW. The unencrypted CW preferably changes at a high rate, for example, once every few seconds. Demultiplexer 230 also selects from transport data stream TDS encrypted service E_{cw} (SERVICE). The encrypted service is processed in decryptor 238 using the CW as the decryption key to recover the unencrypted service.

Detailed Implementation of the Encryption System of FIG. 2: FIG. 3

FIG. 3 presents more details about a preferred implementation of the system of FIG. 2. Encryption/decryption system 301 has two main components: service origination component 305 and service reception component 333. The two are connected by a transmission medium 331, which may be any medium which will carry a message from service origination component 305 to service reception component 333. Service reception component 333 is implemented in a set-top box, termed hereinafter a digital home communications terminal (DHCT). It may, however be implemented in any device which has the necessary computation power, for example, a personal computer or work station or an "intelligent" television set. In the service origination component, at least the portion labeled 306 is typically implemented in equipment located at the head end of a broadcasting system such as a cable television (CATV) or satellite TV system. In some embodiments, however, the head end may be provided with already-encrypted instances of the service. The remaining portion 308 may also be located at the head end, but may also be located anywhere which has access of some kind to head end 306 and service reception component 333. The latter is particularly the case if the EMMs are sent out of band, for example by way of a wide-area network such as the Internet. Also, the transmission medium may be storage media, where the service origination point is the to manufacturer of the media, and the service reception component may be the element which reads the storage media. For example, the transmission medium can be a CD-ROM, DVD, floppy disk, or any other medium that can be transferred, physically, electronically, or otherwise.

Beginning with service origination portion 305, random number generator 307 is used to generate MSK 309. Next, an EMM 315 containing MSK 309 and related information is produced. EMM 315 also includes a sealed digest. The sealed digest has two purposes: to ensure that the information placed in EMM 315 by service origination 305 is the same information that arrives at DHCT 333 and to ensure that the information has in fact come from an entity which is empowered to give access to the service.

The sealed digest is made in two stages: first, a digest of the EMM's contents (here, MSK 309 and the related

8

information) is made by hashing the contents in a secure one-way hash function to produce a relatively short bit string. The secure one-way hash function has three properties:

- the contents that were hashed to produce the short bit string cannot be determined from the short bit string; and
- any change in what is hashed produces a change in the short bit string; and
- it is computationally infeasible to construct a different message which produces the same short bit string as the EMM.

The short bit string output of the hash function can thus be used to determine whether the contents of the EMM have changed in transit without disclosing those contents. The preferred embodiment uses the Message Digest 5 one way hash function, as indicated by the notation MD5. For details on one-way hash functions, see the Schneier reference, supra. The digest is a sealed digest because it is encrypted with a private key SP Kr 310 belonging to the entitlement agent (EA) that has the right to give the DHCT access to the service for which the MSK is used to produce the key. Before the sealed digest can be used to check whether the EMM was transmitted correctly, it must be decrypted using the entitlement agent's public key. The sealed digest thus confirms to the DHCT both that the contents of the EMM have been transmitted correctly and that the source of the EMM is the entitlement agent.

Once the sealed digest is made, the contents of the EMM (here, MSK 309 and the related information) are encrypted with the public key DHCT Ku 312 of the DHCT 333 to which EMM 315 is addressed and EMM 315, containing the encrypted contents and the sealed digest, is sent via transmission medium 331 to the DHCT 333. In the following, the notation Kr is used to indicate a private key and Ku is used to indicate a public key. The notation RSA indicates that the encryption is done using the well-known RSA public key encryption algorithm.

As shown in DHCT 333, EMM 315 can only be decrypted by the DHCT 333 whose private key 337 (DHCT Kr) corresponds to the public key used to encrypt EMM 315. DHCT 333 decrypts EMM 315 and uses the sealed digest to determine whether the EMM 315 was correctly transmitted. The determination is made by using public key SP Ku 335 for the entitlement agent to decrypt the sealed digest. Then the contents of EMM 315 are hashed using the same secure one-way hash function that was used to make the digest. If the results of this hash are identical to the decrypted sealed digest, the determination succeeds. The check with the sealed digest will fail if the transmission to the DHCT 333 was corrupted in transit, if DHCT 333 does not have the private key corresponding to the public key used to encrypt the EMM (i.e., is not the DHCT 333 for which EMM 315 was intended), or if DHCT 333 does not have public key 335 (SP Ku) corresponding to the private key of the EA that was used to make the sealed digest. The latter will be the case if that DHCT 333 has not been given access to services provided by the entitlement agent. EMMs 315 addressed to DHCT 333 are sent repeatedly; consequently, if the problem was corruption in transit, an uncorrupted EMM 315 will be received shortly and the determination will succeed. How DHCT 333 comes to have SP Ku 335 needed to decrypt the sealed digest will be explained in more detail later.

The next stage in service origination 305 is generating control word 319 used to actually encrypt service instance 325 and generating the ECM 323 which carries the information needed to decrypt the service instance to DHCT 333.

The control word 319 is generated by random number generator 317. This can be a true random number generator, whose output is the result of some basic underlying random physical process, or some other means, for example, the result of encrypting a value, called a "counter" (which increments by one after each use) with 3DES, using the MSK as the key. In the case of a true random number, the encrypted control word is transmitted in the ECM. In the case of the counterbased control word generation, the clear version of the "counter" is used in the transmitted ECM. As mentioned above, the control word is a short-term key, i.e., it has a life time of a few seconds or less. Included in the ECM 323 is a digest of the contents plus the MSK which is made using the MD5 one-way hash just described. The inclusion of the MSK in making the digest gives the entitlement agent to which the ECM 323 belongs a shared secret with the DHCTs 333 that are entitled to receive service instances from the entitlement agent and consequently prevents "spoofing" of ECMs 323, that is, provision of ECMs 323 from a source other than the entitlement agent. As will be seen in more detail later, the preferred embodiment uses the shared secret technique generally to authenticate messages which contain messages that have real-time value with regard to an instance of a service.

ECM 323 is sent together with encrypted content 329 to DHCT 333. The first ECM 323 for a given portion of encrypted content 329 must of course arrive at DHCT 333 before the encrypted content does. In the preferred embodiment, content 325 and ECM 323 are encoded according to the MPEG-2 standard. The standard provides for a transport stream which includes a number of component streams. Some of these carry content 329, another carries the ECMs 323, and a third carries the EMMs 315. Only the streams carrying content 329 are encrypted according to DES 329; since the control words in ECMs 323 and the contents of EMMs 315 have already been encrypted, no further encryption is needed when they are sent in the MPEG-2 transport stream. The manner in which EMMs and ECMs are transported in the MPEG-2 transport stream will be described in more detail later.

When an ECM 323 is received in DHCT 333, control word 319 is either decrypted or found by encrypting the counter value at 343 using the MSK. The integrity of the contents of the ECM 323 is checked by comparing the value resulting from hashing the contents plus some or all of the MSK (based on cryptographic principles) in the one-way hash function with the message digest contained in ECM 323. Included in the contents are control word 319 and information identifying the service instance 325 which ECM 323 accompanies. The identifying information is used together with the authorization information received with EMM 315 to determine whether DHCT 333 is authorized to receive the service instance 325. If it is, control word 319 is used in service decryptor 347 to decrypt encrypted content to produce original content 325.

System 301 offers a number of advantages with regard to security. It takes advantage of the speed of symmetrical encryption systems where that is needed to decrypt encrypted content 329 and the control word in ECM 323. The control word is protected by encrypting it using the MSK, and ECM 323 is authenticated by using some or all of MSK 309 as a shared secret between the entitlement agent and DHCT 333. MSK 309 is protected in turn by the fact that it is sent in an EMM which is encrypted using the DHCT's public key and by the fact that the EMM includes a sealed digest which is encrypted using the entitlement agent's private key. Further security is provided by the fact that

service identification information from ECM 323 must agree with the authorization information received in EMM 315 before control word 319 is provided to service decryptor 347. For example, as described in detail in the Banker and Akins parent patent application supra, one use of the information in ECM 323 and EMM 315 is to prevent what are termed "replay attacks" on the encrypted services. In addition to being secure, system 301 is flexible. The authorization information contained in EMM 315 and the service identification information contained in ECM 323 together permit a wide range of access to service instances received in DHCT 333.

Dynamic Provision of Multiple Entitlement agents to DHCT 333: FIG. 4

The use of the sealed digest in EMM 315 means that DHCT 333 will not respond to EMM 315 unless it has a public key for the entitlement agent that has the power to give entitlements to the service to be decrypted by the MSK in EMM 315. This is part of a broader arrangement which makes it possible to dynamically provide DHCT 333 with one or more entitlement agents and to dynamically remove provided entitlement agents from DHCT 333.

The entity which provides and removes entitlement agents is called the conditional access authority (CAA). The arrangement further permits entitlement agents that have been provided to DHCT 333 to dynamically modify their authorization information in DHCT 333. All of the information needed to perform these operations is sent via EMMs, with the sealed digests being used to ensure that only the CAA may add or remove entitlement agents and that only the entitlement agent to which authorization information belongs may modify the authorization information.

The above arrangement has a number of advantages:

It permits multiple entitlement agents.

It permits dynamic addition and removal of entitlement agents.

It places limits on the services to which an entitlement agent may grant entitlements, but otherwise permits entitlement agents to manage their own authorization information.

It separates the business of providing entitlements to services and service instances from the business of actually providing instances of the service; consequently, a CATV operator may simply run as a distribution utility.

It separates the business of giving an entity the right to be an entitlement agent from the business of being an entitlement agent.

It provides an easy way of permitting a customer to change entitlement agents as he or she sees fit.

It provides a secure arrangement whereby a DHCT 333 may communicate by means of a reverse path with an entitlement agent, a conditional access authority, or potentially the provider of the instances of the service.

FIG. 4 shows how the arrangement is implemented in a preferred embodiment. FIG. 4 is best understood as an extension of FIG. 3. Both FIG. 4 and FIG. 3 have the same major components: service origination 305, DHCT 333, and transmission medium 331 for coupling the two. Further, encryptor 313 and decryptor 339 are used in both figures. Moreover, as indicated by reference number 308, the EMMs may be either sent together with a service instance or by another channel. FIG. 4 further shows an additional component of DHCT 333, namely EMM manager 407. EMM manager 407 is implemented in software executed in a secure processor in DHCT 333. The task of EMM manager

407 is to respond to EMMs which add or remove entitlement agents and to EMMs which modify the authorizations for an entitlement agent. EMM manager 407 further provides messages by means of which DHCT 333 may communicate with an entitlement agent or a conditional access authority.

Initially, EMMs that modify an entitlement agent's authorization information are made in response to modification information 403 provided by the entitlement agent or required by the network operator. As shown at 313, the modification information is encrypted using the public key 312 for DHCT 333 and has a sealed digest that is encrypted using the private key 310 for the entitlement agent. The resulting authorization modification EMM 405 is sent via transmission medium 331 to decryptor 339 in DHCT 333, where it is decrypted and checked in the manner described above for EMMs 315 containing an MSK. The EA modification information 403 contained in the EMM goes, however, to EMM manager 407, which uses the information to modify the authorization information for the entitlement agent in DHCT 333. Examples of modifications include adding or canceling services provided by the entitlement authority and changing the conditions under which access to instances of a given service will be granted.

As indicated above, the sealed digest is encrypted using the private key of the entitlement agent. Consequently, the validity of the EMM can only be determined if DHCT 333 has the entitlement agent's public key. The public key for an entitlement agent is provided to DHCT 333 by an EA allocation EMM 413 from a conditional access authority. EMM 413 contains entitlement agent allocation information 409 from the conditional access authority; at a minimum, entitlement agent allocation information 409 contains the public key for the entitlement agent; it may also contain information about the amount of memory an entitlement agent may have in DHCT 333 and about classes of service that an entitlement agent may offer. For example, the entitlement agent may not be permitted to offer interactive services. Information 409 is encrypted with the public key 312 of DHCT 333, and the sealed digest is encrypted with private key 411 of the conditional access authority.

In DHCT 333, EMM 413 is decrypted using private key 337 belonging to DHCT 333 and the sealed digest is decrypted using CAA public key 415. If the digest confirms the correctness of the contents of the EMM, EMM manager 407 allocates storage for the entitlement agent whose public key is contained in EMM 413. That done, EMM manager 407 places the entitlement agent's public key in the storage. The storage provides a place to store the entitlement agent's public key, the authorization information for the services and service instances provided by the entitlement agent, and the MSKs provided by the entitlement agent. Once DHCT 333 has the entitlement agent's public key and storage for the entitlement agent's authorization information and MSK, EMM manager 407 can respond to EMMs from the entitlement agent. Of course, in order to decrypt the sealed digest, DHCT 333 must have public key 415 for the conditional access authority. As will be explained in more detail later on, in a preferred embodiment, public key 415 and the public and private keys for DHCT 333 are installed in DHCT 333 at the time that DHCT 333 is manufactured.

When a customer orders a service, the arrangements just described interact as follows:

1. If the service is provided by an entitlement agent for which the customer's DHCT 333 does not have the public key, the conditional access authority must first send EA allocation EMM 413 to DHCT 333; EMM manager 407 responds by allocating storage for the entitlement agent.

Only the conditional access authority can send EA allocation EMM 413, and consequently, the conditional access authority (CAA) can control access by entitlement agents to customers of a particular service distribution organization.

2. If DHCT 333 has the entitlement agent's public key, either because step (1) has just been performed or was performed at some time in the past, the entitlement agent sends modification EMM 405 with the authorization information for the newly-ordered service or service instance to DHCT 333. EMM manager 407 responds thereto by storing the authorization information in the allocated space.
3. Once step (3) is done, DHCT 333 can receive EMM 315 with the MSK for the service from the entitlement agent. EMM manager 407 stores the MSK in the allocated space.
4. When the actual service instance is sent, it is accompanied by ECMs containing the current control word. The MSK is used to decrypt the ECMs and the control words obtained from the ECMs are used to decrypt the instance of the service.

The above use of EMMs and ECMs to control access to instances of a service thus guarantees that no entitlement agent will have access to DHCT 333 without permission of the conditional access authority and that no DHCT 333 will have access to an instance of a service without permission of the entitlement agent for the service. It also makes it possible for the entitlement agent to be in complete control of the service. Access to the service is defined by the EMMs 405 and 315, and these may be sent by the entitlement agent to DHCT 333 independently of the service distribution organization. Further, it is the entitlement agent which provides the MSK used to generate control words and decrypt the ECM to both the service distribution organization and DHCT 333. Indeed, if the entitlement agent wishes to do so, it can itself provide encrypted instances of the services to the service distribution organization, which, in such a case, merely functions as a conduit between the entitlement agent and DHCT 333.

40 Secure Transmission of Messages Via the Reverse Path

FIG. 4 also shows how the techniques used to ensure the security of EMMs are also used to ensure the security of messages sent from DHCT 333. The example shown in FIG. 4 is a forwarded purchase message (FPM). The forwarded purchase message is used for the interactive purchase of an instance of a service. One example of such a purchase is what is called impulse pay-per-view, or IPPV. In such a system, the beginning of an event, for example, a baseball game, is broadcast generally and customers can decide whether they want to see all of it. In that case, they must provide input to DHCT 333 that indicates that they wish to see the entire event. EMM manager 407 responds to the input by making the FPM and sending it to the entitlement agent so that the entitlement agent can charge the customer for the event and send an EMM 315 confirming that DHCT 333 may continue to decrypt the event. The information needed by the entitlement agent is forwarded entitlement information 417; to ensure the privacy of the customer, this information is encrypted using the 3DES algorithm with a key 420, as shown at 343, to produce encrypted forward entitlement information 419. The key 420 is composed of two 56-bit DES keys. The 3DES encryption operation is a sequence of three DES operations: encryption using the first DES key, decryption using the second DES key, and encryption using the first DES key. Then key 420 is encrypted using the public key 335 of the entitlement agent and the sealed digest is made using the private key of DHCT 333. All of

these parts together make up forwarded purchase message 421, which is addressed to the entitlement agent.

At the entitlement agent, key 420 is decrypted using the entitlement agent's private key 310, and the sealed digest is decrypted using the public key 312 of the DHCT. If the Encrypted Forwarded Entitlement Information (EFEI) 419 contained in the FPM 421 is determined not to have been tampered with, it is passed to 3DES decryption 443, which decrypts it using key 420 and provides forwarded entitlement information 417 to the entitlement agent. As will be immediately apparent, the same technique, with or without the 3DES encryption of the contents of the message, can be used to send messages to any entity for which DHCT 333 has the public key. At a minimum, this includes the CAA and any entitlement agent which has been allocated memory in DHCT 333.

Authentication of Global Broadcast Messages

A global broadcast message is one which is not addressed to any individual DHCT 333 or to any group of DHCTs 333. In a preferred embodiment, global broadcast messages accompany instances of services and contain information that is relevant to the instance they accompany. Consequently, the encryption and authentication techniques used in the global broadcast messages must permit rapid decryption and authenticity checking. One example of a global broadcast message is the ECM. Other examples are the different types of global broadcast authenticated messages, or GBAMs. As with ECMs, it is necessary to prevent global broadcast messages from being spoofed, and it is done in the same fashion as with the ECMs. More specifically, the digest is made using some or all of the MSK together with the content of the global broadcast message. The MSK thus functions as a shared secret between the entitlement agent and DHCT 333. When EMM manager 407 receives the global message, it makes a digest using the contents of the received message and the MSK and responds to the received message only if the digest agrees with the one contained in the message. An advantage of using a digest made with the MSK to authenticate the global broadcast message is that the digest may be both made and checked very quickly.

Implementation of the Conditional Access System in a Digital Broadband Delivery System

The foregoing has described the conditional access system in terms of ECMs, EMMs, and other messages and in terms of the manner in which the messages and their digests are encrypted and decrypted. The conditional access system as just described will work with any communications arrangement which permits an instance of a service to be delivered to a DHCT together with ECMs and other broadcast messages and which permits the DHCT to receive EMMs from a conditional access authority and one or more entitlement agents. The conditional access system is, however, particularly well-suited for use in a modem digital broadband delivery system, and the following will describe how the conditional access system is implemented in such a delivery system.

Overview of the Digital Broadband Delivery System: FIG. 5

FIG. 5 provides an overview of digital broadband delivery system (DBDS) 501. DBDS 501 includes service infrastructure 503, a headend 515, a transport infrastructure 517, hubs 519 (0 . . . n), access networks 521 (0 . . . n), and Digital Home Communications Terminals (DHCTs) 333. The service infrastructure consists of Value-Added Service Provider (VASP) systems 509, which are systems that provide services to the broad band delivery system, the Digital Network

Control System (DNCS) 507, which manages and controls services provided by means of DBDS 501, the Administrative Gateway (AG) 505, which is a source of service provisioning and authorization information in DBDS 501, Network Management System (NMS) 511, which maintains a database of system status and performance information, and the Core Network 513, which interconnects other Service Infrastructure 503 components with headend 515. In a preferred embodiment, Core Network 513 consists of ATM-based switching and transmission facilities. Headend 515 provides an interface between service infrastructure 503 and transport infrastructure 517. Transport infrastructure 517 provides a high-bandwidth interconnection from headend 515 to hubs 519(0 . . . n). Each hub 519(i) serves an access network 521(i), which consists of hybrid fiber coax (HFC) nodes 523 connected via a coax bus network to DHCTs 333. A given DHCT 333(k) in DBDS 501 thus belongs to an HFC node 532(j) in an access network 521(i). Transport infrastructure 517 and access network 523 may provide only a forward channel from head end 515 to a given DHCT 333(k), but preferably provide both a forward channel and a reverse path. Each instance of a DBDS 501 generally provides service to a metropolitan area.

DBDS 501 can be implemented in a variety of configurations to fit the circumstances of a particular service environment. For example, headend equipment may be deployed within headend 515, within a hub 519(i), or as part of a VASP system 509. DNCS components 506 may be deployed within headend 515 or distributed among the hubs 519. Transport infrastructure 517 may utilize SONET add/drop multiplexing, analog fiber technology, or other transmission technologies.

Overview of the Conditional Access System: FIG. 6

FIG. 6 shows the components of a preferred embodiment of conditional access system 601 in DBDS 501. Conditional access system 601 is a collection of components DNCS 507, headend 515, and DHCT 333 that together provide security and conditional access services.

The components of conditional access system 601 perform the following functions:

1. encrypting the service content
2. encrypting the control words used for service encryption
3. authenticating the ECMs that contain the encrypted control words
4. passing the ECMs to DHCTs
5. managing a subscriber authorization database
6. encrypting and authenticating EMMs containing subscriber entitlement information
7. passing the EMMs to DHCTs
8. decrypting the EMMs and checking their authenticity at the DHCTs
9. responding to the EMMs by modifying entitlement information in the DHCTs
10. responding to the ECMs by authenticating them, decrypting the control word, and checking entitlement at DHCT 333, and
11. if the ECM is authentic and the authorizations permit, decrypting the service content.

These requirements are met by the following components of conditional access system 601:

- Stream Encryption & ECM Streamer Modules 620 in head end 515;
- Control Suite 607 in DNCS 507;
- I. Transaction Encryption Device 605 in head end 515, with secure link to DNCS 507;
- II. Service Decryptor Module 625 in DHCT 333;

III. Security Manager Module 626 in DHCT 333; and
IV. DHCTSE 627 in DHCT 333.

FIG. 6 depicts a typical configuration of these components for securing digital services within DBDS 501. In the following, the components will be described in more detail. Service Encryption & ECM Streamer Module 620

Service Encryption and ECM Streamer (SEES) module 620 is a component of QAM Modulator 619 that operates under direction of control suite 607 to encrypt the MPEG-2 transport stream packets that are employed in the preferred embodiment to transmit service content 325. As shown in FIG. 6, service content 325 may be received from sources such as a digital satellite distribution system 613, a digital terrestrial distribution system 611, or a media server 609. Media server 609 may be connected to head end 515 by a broadband integrated gateway 615. SEES 620 uses MSK 309 to generate the control words 319 used for service encryption and creates ECMs 323 for transporting the control words together with encrypted service content 329 within the outgoing MPEG-2 Transport Stream. SEES 620 encrypts the control words in the ECMs 323 with MSKs 309. The MSKs are generated by TED 603 and are sent to SEES 620 in encrypted form in EMM-like messages. DHCT 333

DHCT 333 is connected between the HFC network 521 and the customer's television set. DHCT 333 receives and interprets EMMs, ECMs, and GBAMs and decrypts instances of services. DHCT 333 further provides the customer interface for DBDS 501 and receives customer input 628 from the customer. In response to the customer input, DHCT 333 may generate FPMs or other messages that travel via the reverse path to the CAA or to EAs. In a preferred embodiment, DHCT 333 is implemented using a combination of general purpose processors, ASICs, and secure elements (which may be implemented discretely or integrated). For purposes of the present discussion, DHCT 333 has three important components: service decryption module 625, security manager 626, and DHCT secure element (DHCTSE) 627. Service decryption module 625 is preferably implemented in an ASIC, and security manager 626 is preferably implemented in software. DHCTSE 627 is a secure element for performing security and conditional access-related functions.

Service Decryptor Module 625

Service decryptor module 625 is the component of DHCT 333 that decrypts the encrypted MPEG-2 transport stream packets. Service decryptor 625 receives the control words to be used for service decryption from DHCTSE 627. DHCTSE 627 controls which transport stream packets are decrypted by only passing the control words for authorized services to service decryptor 625.

Security Manager 626

Security manager 626 is a software module of the DHCT that provides an interface between applications running on DHCT 333 which use the conditional access system and DHCTSE 627. It also coordinates processing between the service decryptor module and DHCTSE 627.

DHCTSE 627

DHCTSE 627 stores keys, interprets EMMs and ECMs, and produces FPMs. With the EMMs and ECMs, it does the decryption and authentication required for interpretation and with FPMs, it makes the sealed digest and encrypts the FPM. Thus, in the preferred embodiment, EMM manager 407 is implemented in secure element 617. In addition, DHCTSE 627 provides encryption, decryption, digest, and digital signature services for other applications executing on DHCT 333. Secure element (DHCTSE) 627 includes a micropro-

cessor and memory that only the microprocessor may access. Both the memory and the microprocessor are contained in tamper-proof packaging. In interpreting EMMs, DHCTSE 627 acquires and stores keys and entitlement information; in interpreting ECMs, DHCTSE 627 uses the entitlement information to determine whether DHCT 333 receiving the ECM has an entitlement for the instance of the service which the ECM accompanies; if it does, DHCTSE 627 processes the ECM, and provides the control word to service decryptor module 625 in a form that it may use to decrypt or descramble services. DHCTSE 627 further records purchase information for impulse-purchasable services such as IPPV and stores the purchase data securely until the data is successfully forwarded via a forwarded purchasing message to control suite 607. DHCTSE 627 maintains MSK for the EAs, the private/public key pairs for DHCT 333, and the public keys of the conditional access authorities and the entitlement agents.

Control Suite 607

Control suite 607 is a member of the DNCS family of software. Control suite 607 controls the encryption of services performed by a SEES module 620 based upon input from the DNCS broadcast control suite component. Control Suite 607 also maintains a database of subscriber authorizations based upon transactions received from Administrative Gateway 511. Control suite 607 generates EMMs for communicating subscriber authorizations and other conditional access parameters to the DHCTSE 627. Control suite 607 acts on behalf of entitlement agents. The EMMs generated by control suite 607 for communicating subscriber authorizations and other conditional access parameters to DHCTSE 627 are encrypted with the public keys of the DHCTs 333 to which they are directed and are authenticated with the private key of the EA, which is maintained by transaction encryption device (TED) 603. DHCTSE 627 maintains the public key of the EA and uses it to confirm the authenticity of EMMs generated by control suite 607 for the EA.

Control Suite 607 further enables the establishment of a conditional access authority (CAA). Control suite 607 generates EA allocation EMMs 413 which pass the public key of the EA to a DHCTSE 627. These EMMs 413 are encrypted as described above, but are authenticated using a digital signature made with the private key of the CAA, which is maintained by TED 603. DHCTSE 627 is pre-provisioned with the public key of the CAA for use in confirming the authenticity these EMMs 413.

Communications between control suite 607 and the rest of conditional access system 601 are by means of LAN interconnect devices 605 and 617. Device 605 connects Control Suite 607 to Administrative Gateway 505, from which it receives the information necessary to make ECMs and EMMs, and device 617 connects it to the SEES modules 620 in the QAM modulators and to QPSK modulator 621 and QPSK demodulator 623, which are in turn connected to HFC network 521. The connection between Control Suite 607 and DHCT 333 via LAN interconnect device 617, modulator 621, demodulator 623, and HFC network 521 implements the reverse path needed for messages such as FPM 421 and also implements a forward channel to DHCT 333. This forward channel is independent of the forward channel used to provide the services. In conditional access system 601, Control Suite 607 can send FPMs or broadcast messages to DHCT 333 either by the forward channel just described or by sending them together with an instance of a service.

Transaction Encryption Device 603

Transaction Encryption Device (TED) 603 serves as a peripheral to Control Suite 607. TED 603, under the direc-

tion of Control Suite 607, encrypts and makes sealed digests of various conditional access system messages, including EMMs. TED 603 may also generate and store (MSKs) which are used by SEES 620 to encrypt the control words in the ECMs and to decrypt the control words in DHCTSE 627. TED 603 further uses the MSKs to authenticate the global broadcast message class of conditional access system messages. Authentication is done by hashing the contents of the message together with some or all of the MSK. TED 603 decrypts and verifies the authenticity of Forwarded Purchase Messages 421 sent from the DHCTs 333 as well as other messages sent using the reverse path. TED 603 maintains the private keys of the CAA and the EA and receives from the DNCS the public keys of the DHCTs from which it receives messages. As will be explained in more detail below, TED 603 receives the public keys from a source that confirms the authenticity of each key. TED 603 finally makes a sealed digest for the EMMs using the private key of the CAA and EA as appropriate for the EMM.

Using the Conditional Access System to Support Services and Programs Executing in DHCT 333 or Service Infrastructure 507

The conditional access system can be utilized to secure the provisioning of a service or to provide security services to programs executing on DHCT 333 or programs in Control Suite 607. Secure service provision does not require that the DHCT programs that support the service be secure. The reason for this is that the following may be done only by DHCTSE 627 in DHCT 333 or by a TED 603:

- generation of the MSK;
- storage of the MSK;
- storage of the keys needed to encrypt and/or decrypt EMMs and to make and check sealed digests;
- storage of the entitlement information received from the EAs;
- encryption and/or decryption of EMMs;
- encryption or decryption of the control word;
- provisioning of the MSK to SEES module 607 and the decrypted control word to service decryption module 625;
- making and checking digests with shared secrets;
- making and checking sealed digests;
- confirming that a DHCT 333 is entitled to receive a service.

A program executing on DHCT 333 or a program in control suite 607 has no access to any of the information stored in DHCTSE 627 or TED 603 and can thus do nothing with EMMs and ECMs beyond asking DHCTSE 627 or TED 603 to generate or interpret them. For example, when DHCT 333 receives an EMM, it simply passes the EMM to DHCTSE 627 for processing; when it receives an ECM, it does the same; if the authorization information contained in the FCM and stored in the DHCTSE 627 indicates that DHCT 333 is entitled to the service, DHCTSE 627 provides the decrypted control word to service decryption module 625.

The conditional access system can also do security checking for programs generally. For example, a program executing on DHCT 333 that requires downloaded information from a server application may expect that a sealed digest was added to the information before it was downloaded, and the program may use DHCTSE 627 to check the sealed digest and determine whether the information is authentic, but it is up to the program to decide what to do with the information when DHCTSE 627 indicates that it is not authentic.

Details of Messages in Conditional Access System 601

In conditional access system 601, the ECM, the EMM, the FPM, and the GBAM are all different types of conditional access messages. The conditional access messages all have a common format, namely a header, the message itself, and a message authentication code, or MAC. The header contains the following information:

- the type of the message, i.e., whether it is an ECM, EMM, GBAM, or something else;
- the length of the message;
- an identifier for the conditional access system;
- an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents; and
- the length of the message content.

The header is followed by the encrypted message and the MAC, which, depending on the message type, may be a sealed digest or a digest made with some or all of the MSK together with the message.

In digital broadband delivery system 501, CA messages may travel either in a MPEG-2 data stream or in an IP packet, that is, a packet made according to the rules of the Internet Protocol. Also, other transport protocols such as ATM may be used. In the preferred embodiment, messages from control suite 607 to DHCT 333 may travel in MPEG-2 or IP packets; messages from DHCT 333 to control suite 607 travel as IP packets on the reverse path provided by QPSK demodulator 623 and LAN interconnect device 617. In general, messages to DHCT 333 which are closely associated with particular instances of services, such as ECMs and GBAMs, travel in the MPEG-2 data stream; EMMs may travel either in the MPEG-2 transport stream or as IP packets via LAN interconnect device 617 and QPSK modulator 621. CA Messages in the MPEG-2 Transport Stream: FIG. 7

FIG. 7 is a schematic representation of an MPEG-2 transport stream 701. An MPEG-2 transport stream is made up of a sequence of 188-byte long transport packets 703. The packets 703 in the stream carry information that, when combined at DHCT 333, defines an instance of a service and the access rights of a given DHCT 333 to the service. There are two broad categories of information: program 709, which is the information needed to produce the actual pictures and sound, and program specific information (PSI) 711, which is information concerning matters such as how the transport stream is to be sent across the network, how the program 709 is packetized, and what data is used to limit access to the program 709. Each of these broad categories has a number of subcategories. For example, program 709 may include video information and several channels of audio information.

Each transport packet 703 has a packet identifier, or PID, and all of the packets 703 that are carrying information for a given subcategory will have the same PID. Thus, in FIG. 7, the packets carrying Video 1 all have PID (a), and the packets belonging to that subcategory are identified by 705(a). Similarly, the packets carrying Audio 1 all have PID (b), and the packets belonging to that category are identified by 705(b). A subcategory of information can thus be identified by the PID of its packets. As shown at output packets 707, the output from mux 704 is a sequence of contiguous individual packets from the various subcategories. Any part or all of MPEG-2 transport stream 701 may be encrypted, except that packet headers and adaptation fields are never encrypted. In the preferred embodiment, the sets of packets making up program 709 are encrypted according to the DES algorithm, with the control word as a key.

Two of the subcategories are special: those identified by PID 0 (705(e)) and PID 1 (705(c)) list the PIDs of the other packets associated with the service(s) and thus can be used to find all of the information associated with any service. The packets in PID 1 705(c) have as their contents a conditional access table 710, which lists the PIDs of other packets that contain EMMs. One set of such packets appears as EMM packets 705(d), as indicated by the arrow from CAT 710 to packets 705(d). Each packet 703 in packets 705(d) contains private information, that is, information which is private to conditional access system 601. As will be explained in more detail below, private information 713, for the purposes of this invention, is a sequence of CA messages, each of which contains an EMM, and private information 719, is a sequence of messages, each of which contains an ECM.

The packets in PID 0 705(e) contain a program association table which lists PIDs of packets that are associated with a particular instance of a service. One such set of packets is program maps packets 705(f), which contain a program map table 717 that lists, amongst other things, the PIDs of transport packets 703 containing ECMs for the program. One such set of packets is shown at 705(g). Each of the transport packets contains private information 719, which in this case is a sequence of CA messages, each of which contains an ECM.

FIG. 8 shows in detail how EMMs are carried in transport packets 703. The payload space 719 in the packets carries data from a CA_PRIVATE_SECTION layer 803, which in turn contains a sequence of CA messages 805, each of which contains an EMM 807. In the sets of packets 705(g) carrying ECMs, the control words in the ECMs are encrypted using the 3DES algorithm with the MSK as key; in the sets of packets 705(d) carrying EMMs, the EMMs are encrypted using the public key of DHCT 333 for which they are intended. As will be immediately apparent, the techniques just described can be employed to transmit any CA message 805 as part of an MPEG-2 transport stream.

Mapping CA Messages into IP Protocol Packets: FIG. 9

FIG. 9 shows how EMMs are mapped into the Internet Protocol (IP) packets used to communicate between control suite 607 and DHCT 333 via LAN device 617 and QPSK modulator 621 and demodulator 623. An IP packet 903 is a variable-length packet that consists simply of a header and a payload. The header contains source and destination IP addresses for the packet. With an EMM, the source address is the IP address of the CA or EA, and the destination address is the IP address of DHCT 333. In the preferred embodiment, the IP address of DHCT 333 is constructed using its serial number. The IP addresses in DBDS 501 are partitioned by HFC node 523. The payload of the IP packet is a packet 905 belonging to the User Datagram Protocol (UDP) which has as its payload a CA_PRIVATE_SECTION 803, which in turn contains a sequence of CA messages 805, each of which contains an EMM 807.

ECM Structure Details: FIG. 10

FIG. 10 shows details of the structure of an ECM 1008 and shows the mapping 1001 from an ECM 1008 to a set 705(c) of MPEG-2 transport packets 703. As before, the data of a CA_PRIVATE_SECTION 803 is carried in a set of MPEG-2 transport packets 703 with the same PID. The data is a header 1003 for private section 803 and a sequence of CA messages 805, each of which includes a CA message header 1005, a CA ECM message 1007, and an ECM MAC 1013. CA ECM message 1007 and ECM MAC 1013 together make up ECM 1008.

FIG. 10 also shows how the control word is protected in ECM 1008 and how ECM MAC 1013 is produced. The

control word is a random value that is either encrypted using 3DES encryption or created by encrypting a counter value using 3DES encryption, using the MSK as the key. In either case, the preferred embodiment calls for an MSK which is made up of two 56-bit DES keys, and the 3DES encryption operation is a sequence of three DES operations: encryption using the first DES key, decryption using the second DES key, and encryption using the first DES key. The control word, too, may have even or odd parity. As shown at 1013, the odd control word (after suitable encryption) becomes part of ECM_entitlement_unit_message 1011, and, in its non-encrypted form, is used together with some or all of the MSK as input to the MD5 one-way hash function to produce ECM MAC 1013. The same procedure is used with the even-parity control word. The contents other than the control word of ECM_entitlement_unit_message 1011 will be examined in more detail later.

EMM Structure Details: FIG. 11

FIG. 11 shows a CA message 805 which contains an EMM 1112. CA message 805 has a header 1003, a CA EMM message 1101, and a sealed digest 1103. CA EMM message 1101 consists of CA EMM message header 1105, EMM message 1107, and CRC error detection code 1109. EMM message 1107 in its turn contains EMM header 1113 and EMM_inside_data 1115. EMM_inside_data 1115 is encrypted using the public key of the DHCT 333 for which it is intended. The data which is encrypted is EMM data 1129, which in turn is made up of EMM_inside_header 1123 and EMM command_data 1125 together with padding 1127. EMM data 1129 is also input to the MD5 one-way hash function to produce EMM MAC 1119 and sealed digest 1103 is made by encrypting EMM_signing_header 1117, EMM MAC 1119, EMM_signing_header 1117, and padding 1121 with the private key of either an entitlement agent or a conditional access authority, depending on what kind of EMM it is.

The EMM_signing_header is information from the EMM_inside_header. This information is particularly sensitive and is consequently encrypted by both the public key of DHCT 333, for privacy reasons, and the private key of the entitlement agent or the conditional access authority, to apply a digital signature. Upon reception, and after the privacy decryption, if the signature verification fails, the EMM is discarded by DHCT 333. Included in this information are an ID for the conditional access system, the type of the CA message, the serial number of the microprocessor in the DHCT's DHCTSE 627, an identifier for the CAA or EA which is the source of the EMM, an indication of which of the three public keys for the CAA in DHCT 333's secure element is to be used to decrypt the sealed digest, and an indication of the format of the EMM. The contents of EMM command_data 1125 will be explained in more detail in the discussion of the operations performed using EMMs.

Details of DHCTSE 627: FIGS. 12-14

DHCTSE 627 has five main functions in conditional access system 601:

- It securely stores keys including the public and private keys for DHCT 333, public keys for the CAA, public keys for EAs from which DHCT 333 is authorized to receive services, and MSKs provided by those EAs.
- It securely stores entitlement information sent by the EAs.
- It decrypts, authenticates, and responds to EMMs.
- It decrypts the control words in the ECMs, authenticates the ECMs, and when DHCT 333 is authorized to receive the service instance to which the ECM belongs, it provides the control word to service decryptor 625.
- It provides encryption, decryption, and authentication services to applications running on DHCT 333.

DHCTSE 627 includes a microprocessor (capable of performing DES), specialized hardware for performing RSA encryption and decryption, and secure memory elements. All of the components of DHCTSE 627 are contained in a single tamper-proof package such as a package that upon attempting to access the information contained within the information is destroyed. Only the components of DHCTSE 627 have access to the information stored in the secure memory elements. Any attempt by a user to gain access to any of the parts of DHCTSE 627 renders DHCTSE 627 unusable and its contents unreadable. DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a "smart card". The user "personalizes" the DHCT 333 by installing the module in it.

FIG. 12 provides an overview of the components of DHCTSE 627. As shown, the components of DHCTSE 627 are all connected to a bus 1205. Beginning with interface 1203 to the general purpose processor upon which applications execute in DHCT 333, interface 1203 permits passage of data between the remaining components of DHCT 333 and DHCTSE 627, but does not permit components in the remainder of DHCT 333 to address and read the contents of secret values in memory in DHCTSE 627. Microprocessor 1201 executes the code for doing encryption, decryption, and authentication and interpreting EMMs and ECMs; RSA hardware 1217 is special hardware performing the calculations involved with RSA encryption and decryption.

Memory 1207 contains the code executed by microprocessor 1201, the keys, and the entitlement information. In a preferred embodiment, there are two kinds of physical memory in memory 1207: ROM 1219, which is read-only memory whose contents are fixed when DHCTSE 627 is manufactured, and non-volatile memory (NVM) 1209, which can be read and written like normal random-access memory, but which retains its current values when DHCTSE 627 is without power. Non-volatile memory 1209 is organized as a set of non-volatile storage cells (NVSCs) 1211 (0 . . . n), as described in U.S. Pat. No. 5,742,677, Pinder, et al., Information Terminal Having Reconfigurable Memory, filed Apr. 3, 1995.

As will be explained in greater detail below, code executing in microprocessor 1201 dynamically allocates NVSCs 1211 to entitlement agents. In the preferred embodiment, NVM 1209 is used for the storage of information which can be rewritten by means of EMMs, and ROM 1219 is used for code which will not change during the life of DHCTSE 627.

FIG. 13 is a schematic overview of the contents of memory 1207 in DHCTSE 627. The memory is divided into two main parts: read-only storage 1301, which contains code and other information that does not change as a result of the interpretation of EMMs, and NVA storage 1303, which is non-volatile storage that changes as a result of the interpretations of EMMs. RO storage 1301 contains code 1305.

Code 1305 falls into four categories: code 1307 for the encryption, decryption, and authentication operations performed by DHCTSE 627, code for interpreting EMMs 1313, code for interpreting ECMs 1321, and code for handling other CA messages such as the FPM and the GBAM. Code 1307 includes code 1308 for the MD5 one-way hash algorithm, the code 1309 for the RSA public key algorithm, and the code 1311 for the 3DES algorithm. EMM code 1313 falls into three classes: code 1315 which interprets EMMs received from a conditional access authority, code 1317 which interprets EMMs employed by the entitlement agents to configure the storage allocation they receive from the CAA, and code 1319 which interprets EMMs containing MSKs and entitlements. Code 1315, 1317 and 1319 thus

implements EMM manager 407 in a preferred embodiment. The code for interpreting ECMs 1321 decrypts the control word contained in the ECM and checks whether DHCT 333 is permitted to access the instance of the service that the ECM accompanies; if so, the code provides the decrypted control word to service decryption module 625. The code for other CA messages 1323 deals with messages such as the FPM and GBAM.

NVA storage 1303 has two main components: administrative storage 1330 and EA storage 1331. Administrative storage 1330 contains DHCT keys 1325, CAA keys 1329, and CAA data 1330. Beginning with DHCT keys 1325, each DHCT 333 has two public-private key pairs. The public key of one of the pairs serves as the public key used to encrypt EMMs sent to DHCT 333, and the private key is used in DHCT 333 to decrypt the messages; the private key of the other of the pairs is used to encrypt the sealed digests of messages sent by DHCT 333, and the public key is used by other network elements to decrypt the sealed digests of messages received from DHCT 333. The pairs of keys are installed in DHCTSE 627 when DHCTSE 627 is manufactured.

In a preferred embodiment, the manufacturer of DHCT 333 maintains a certified database which has the serial number of each DHCT together with the pair of public keys belonging to it. When a CAA or EA wishes to begin sending EMMs to a DHCT 333, it sends a message to control suite 607 with the serial number of the DHCT. Control suite 607 responds to the request by requesting the public key for the DHCT from a database maintained by the manufacturer of DHCT 333. The database responds to the message by sending control suite 607 certified copies of the public keys for the DHCT. The manufacturer thus functions as the certification authority for the keys. Control suite 607 stores the public keys in a database of its own. For details on key certification, see Schneier, *supra*, pages 425-428. Getting the public keys for the DHCT from the manufacturer has two advantages: first, it solves the problem of certifying the keys; second, because the public keys come from the manufacturer and not from DHCT 333, there is no requirement in conditional access system 601 that DHCT 333 have a reverse path to control suite 607.

CAA keys 1329 are public keys for the conditional access authority. In a preferred embodiment, CAA keys 1329 include three public keys for the conditional access authority. These keys are originally installed when DHCTSE 627 is manufactured, but may be changed in response to EMMs, as will be explained in more detail below. CAA data 1330 includes parameters used by the CAA in managing EA storage 1331, and maps which map NVSCs belonging to particular entitlement agents to 8-bit names and thereby permit the CAA and the entitlement agents to manipulate the NVSCs 1211 by name.

Entitlement agent 1331 has EA information 1331 for each entitlement agent from which DHCT 333 containing DHCTSE 627 can obtain services. The CAA uses EMMs to allocate NVSCs 1211 for an entitlement agent and the entitlement agent then uses EMMs to set the contents of its entitlement agent information 1333.

FIG. 14 shows how NVSCs 1211 are organized into EA storage 1331 in a preferred embodiment. There are two kinds of NVSC's 1211: "skinny" NVSCs, as shown at 1405, and "fat" NVSCs, as shown at 1409. A fat NVSC is made up of a number of skinny NVSCs. The storage 1403, which contains the three CAA public keys, also contains two pointers: one, 1402, to a free list 1407 of unallocated skinny NVSCs and the other, 1404, to an entitlement agent list 1406

of allocated fat NVSCs 1409. There is such a fat NVSC 1409(i) for each entitlement agent from which DHCT 333 may receive services. Each of these NVSCs 1409(i) may also have a list 1411 of NVSCs, which may be skinny NVSCs 1405, fat NVSCs 1409, or a combination of both. A given NVSC 1409(i) and its list of skinny NVSCs make up EA information 1333(i) for an EA. The fat NVSC 1409 is an EA descriptor. As shown at 1333(i), the skinny NVSCs 1411 contain information for the services provided by the entitlement agent such as an MSK for a service, a bit map of entitlement information, and information needed for interactive services such as IPPV.

Control of NVA Storage 1303

In a preferred embodiment, allocation and de-allocation of the NVSCs 1211 may be ultimately controlled by either the CAA or DHCTSE 627. When the CAA controls allocation and de-allocation, the CAA, usually representing the operator of DBDS 501, negotiates with each of the entitlement agents and agrees on an allocation of the various types of NVSCs for that entitlement agent. EA administrative code 1317 checks when it is interpreting EMMs from an entitlement agent to ensure that the entitlement agent does not use more NVSCs of each type than those allocated to it.

When DHCTSE 627 controls NVA storage 1303, the operator of the CAA negotiates with each of the service providers and agrees on the allocation of storage needed for the services provided. The CAA then sends an encrypted message to the entitlement agent. The encrypted message contains the allocation based on data types, and the entitlement agent prevents the service provider from asking for more resources than were negotiated. If DHCTSE 627 nevertheless receives requests for storage area above what is available in NVA 1303, it indicates to the user of DHCT 333 via the user interface that no more storage is available and requests the user to either remove some service provider resources or to rescind the request.

Details of Operations Specified by EMMs

In the following, examples of operations specified by EMMs will be given, beginning with changing a CAA public key, continuing through establishing an EA in DHCTSE 627, and ending with providing entitlement information for broadcasts, events, and interactive services. In the preferred embodiment, a single CAA controls the allocation of EA storage 1331 to entitlement agents. In other embodiments, there may be more than one CAA. There are two kinds of entitlement information: that for broadcast services and that for interactive services. Storage for broadcast entitlements is more permanent than that for interactive entitlements.

The amount of memory 1207 in DHCTSE 627 is limited. The CAA manages this scarce resource and allocates it to the entitlement agents from which DHCT 333 receives services. Different EAs may have different amounts of storage area allocated, depending on their needs. Once an EA has received an allocation from the CAA, the EA may configure the storage area within limits defined by the CAA. Different EAs may have different limits and different types of limits. At one extreme, the CAA only restricts the total number of NVSCs 1211 that an EA may have in its EA information 1333. The CAA may impose tighter restrictions by limiting the types of NVSCs 1211 and/or the number of each type. In this way, the CAA can prevent the EA from offering specific kinds of services and can limit the amount of such services offered, i.e., the amount of time that such services are offered.

When a CAA allocates fat and skinny NVSCs 1211 for an EA, it gives each allocated NVSC 1211 a "name", i.e., each NVSC 1211 has an identifier, such as an 8-bit identifier, that

the CAA associates with the EA for which it has allocated the NVSCs 1211. The CAA and the EA use the name for the NVSC 1211 to refer to it in EMMs that manipulate the NVSC. An NVSC's name need not have anything to do with its physical location in NVM 1209. Since the name space is 8-bits wide, the names are assigned using a 256-bit map. If an entitlement agent has the name of an NVSC, it may make the NVSC into any type of NVSC as long as the type is one that is permitted for the EA and as long as the total number of NVSCs of the type belonging to the EA does not exceed the limit set by the CAA that authorized the EA.

Once the CAA has allocated the EA storage area in the DHCTSE, it is up to the EA to configure the storage area. The first step is to load certain parameters such as a PIN into a descriptor for the EA. The second step is to determine which types of NVSCs are to be used for the protected services to be offered. The names allocated by the CAA are then distributed among the various types of NVSCs. Lastly, each NVSC is loaded by sending the appropriate EMM.

Addressing EMMs

In the conditional access layer, EMMs are addressed to a specific DHCTSE 627, indexed by CAA or EA. This indexing is taken care of in EMM header 1113, which includes a unique identifier for the CAA or EA that is the source of the EMM, and that therefore is associated with the private key used to make the EMM's scaled digest. The EMM header also includes the serial number for DHCTSE 627. The DHCTSE 627 responds only to those EMMs that include its serial number. When a CAA is the source of the EMM, there is also a value in the header indicating which of the CAA public keys is the public key for the source of the message. Conditional access messages may be transported in other data protocols, which may include other addressing mechanisms.

DHCTSE 627 ignores EMMs that are addressed to a CAA or EA that is not "known" by DHCTSE 627 (i.e., EMMs for which there is no CAA corresponding to the CAAID or EA that corresponds to the EAID). As will be explained in more detail below, information about individual entitlements is contained in NVSCs 1211 for the entitlements. Each of these NVSCs has a type, and an EA may change the type or contents of an NVSC 1211 by sending an EMM which specifies the name of the NVSC 1211 to be altered. DHCTSE 627 will alter the NVSC 1211 as indicated in the EMM unless the entitlement agent does not have an NVSC with that name or the change violates a constraint set by the CAA. In those cases, the EMM is ignored by DHCTSE 627. Conditional access system 601 does not require that digital broadband delivery system 501 have a reverse path, or, if one exists, that any bandwidth on the reverse path be available to the EMM conditional access function. Consequently, DHCT 333 does not return any acknowledgment, confirmation, or error messages in response to an EMM. Therefore, the CAA or EA that is the source of an EMM should track the allocations of NVSCs 1211 and send only EMMs that request legal operations. In other embodiments, a reverse path may be required, and for these embodiments, the reverse path can be used for acknowledgment or error messages.

Changing a CAA

As previously indicated, a CAA is represented in DHCTSE 627 by its public key. Three public keys for the CAA are installed in DHCTSE 627 when it is manufactured. A need may occasionally arise to change the CAA of DHCTSE 627. One circumstance under which such a need would arise would be if the private key for the CAA had been compromised; another would be if a new entity has

taken over the function of authorizing entitlement agents. That might happen, for example, as a consequence of the sale of all or part of a DBDS 501.

Any one of the public keys for a CAA can be replaced by means of a sequence of two EMMs, the first of which has a sealed digest encrypted with the private key corresponding to a first one of the other two public keys, and the second of which has a sealed digest encrypted with the private key corresponding to the second one of the other two private keys. Each of the two EMMs contains an identifier, the CAAID for the new CAA, a key select value indicating which of the three CAA public keys is to be replaced, and the public key for the new CAA. After the first EMM is successfully authenticated by DHCTSE 627 by verifying the digital signature applied by the first CAA key, DHCTSE 627 computes a MD5 hash of the new CAA public key in this first EMM and stores it. After the second EMM is successfully authenticated by the DHCTSE by verifying the digital signature applied by the second CAA key, the DHCTSE computes a MD5 hash of the new CAA public key included in this second EMM. This second hash is compared with the first. If the hashes are identical, the new CAA public key and CAAID are substituted for the public key and CAAID of the CAA specified by the key select value. A single CAA public key must not be changed twice without one of the other two CAA public keys being changed in between.

Dynamically Adding and Removing Entitlement Agents in DHCTSE 627: FIG. 15

When a CAA authorizes a DHCT 333 to receive services from an entitlement agent, it does so by sending a sequence of EMMs that create an entitlement agent descriptor EAD 1409 for the new entitlement agent. FIG. 15 shows a detailed view of an EAD 1409(z) as created by the CAA EMMs. Header 1502 is common to all NVSCs 1211. Cell status 1501 indicates whether the NVSC 1211 is allocated. Cell type 1503 indicates what kind of data it contains; with an EAD 1409. Cell type 1503 indicates that the cell is a "fat" NVSC. Cell name 1505 is the 8-bit name that the CAA gives the cell when it allocates it. The names are per-EA. That is, the EA information 1333 for an EA may include up to 255 NVSCs. Next element 1507 is a pointer to the next element in the list to which the NVSC belongs. Thus, in an unallocated NVSC, it is a pointer to the next NVSC in free list 1407; in an EAD 1409, it is a pointer to the next element in EAD list 1406, and in a skinny NVSC that is part of a list 1411, it is the next skinny NVSC in that list. Next element 1507 is set in response to whatever EMM causes the list to be manipulated.

The remaining fields are particular to EADs 1409. The fields labeled 1506 in FIG. 15 are all set by EMMs from the CAA. EAID 1509 is an identifier for the entitlement agent to which EAD 1409 belongs; in the preferred embodiment, EAID 1509 is used to locate EAD 1409 for a given entitlement agent. CAA flags 1511 are a set of flags that indicate (1) the classes of service to which the entitlement agent can grant access and (2) whether the public key for the entitlement agent is installed in EAD 1409. First skinny NVSC 1513 is a pointer to skinny NVSC list 1411 belonging to EA information 1333 to which EAD 1409 belongs. EA maximums 1515 define the maximum amounts of services for the EA to which EA information 1333 belongs. The last field 1506 set by the CAA is EA public key 1527, which is the public key for the EA to which EA information 1333 belongs.

The fields in EA fields 1516 contain information that is associated with the customer to whom DHCT 333 belongs. The fields are set by an EMM received from the EA after

EAD 1409 has been allocated and fields 1506 have been set. DHCT flags 1517 include flags indicative of the services provided by the EA that this specific DHCT 333 is presently entitled to receive. Stored credit limit field 1519 is used with instances of impulse services, i.e., instances of services that need not be purchased in advance. Stored credit limit field 1519 indicates the maximum amount of a service that an interactive customer can use without authorization from the EA. As will be explained in detail below, authorization is obtained by sending an FPM to the EA and receiving a confirming EMM from the EA. X coordinate 1521 and Y coordinate 1523 define a location of DHCT 333 in a coordinate system (to be explained more fully later) established by the entitlement agent. The coordinate system may be geographic and may, for example, be used to determine whether the DHCT 333 is in an area which is to be blacked out in a broadcast. The coordinate system may also be used generally to define subsets of an EA's customers. For instance, the X coordinate and Y coordinate could be used to define customers who do not wish to receive movies that have ratings other than G or PG-13. The PIN is a multi-character code that the customer for the DHCT uses to identify himself or herself to the entitlement agent.

The EMMs that the CAA sends to set up EA information 1333 for an EA are the following:

- Set EA Allocation Name Map
- Set EA Maximum Allocations
- Update Entitlement Agent Public Key

EMM header 1113 in all of these EMMs contains a CAAID for the CAA, and all of the EMMs have a sealed digest that has been encrypted with the CAA's private key. The CAA may use these EMMs not only to set up EA information 1333, but also to modify already existing EA information 1333 for an EA and to remove EA information 1333 for an EA. When the latter has been done, DHCTSE 627 will no longer respond to EMMs or ECMs from the entitlement agent.

Set EA Allocation Name Map

The Set EA Allocation Name Map EMM contains an EAID, which uniquely identifies the EA for which the EA information 1333 is being created or modified, and a name map. The map has a bit for each name; when the CAA has allocated a NVSC for the EA, the bit corresponding to the NVSC's name is set. CAA EMM code 1315 responds to this EMM by allocating the NVSCs required for EA information 1333, mapping the names for the EAID to the physical locations of NVSCs, making list 1411 and setting first NVSC flag 1513 to point to it, adding the new EA Descriptor 1409 to the head of EA list 1406 and setting next element pointer 1507 accordingly, and filling out header fields 1502 and EAID field 1509.

CAA EMM code 1315 stores the current name map for the EA in CAA data 1330 and consequently can compare the name map in a newly-received Set EA Allocation Name Map EMM with the current name map. If a name is specified in both name maps, the Set EA Allocation Name Map command does not affect the NVSC 1211 with the name. If the name map in the EMM specifies a name that was not in the current name map, an NVSC 1211 corresponding to that name is added to list 1411. If the name map in the EMM no longer specifies a name that was previously allocated to the entitlement agent, the NVSC 1211 corresponding to that name is returned to free list 1407. After this is done, the name map in the EMM becomes the current name map.

Typically, an entitlement agent and a conditional access authority will cooperate in determining how large list 1411 should be. For example, if an entitlement agent needs less

space. it will send a message to that effect to the CAA, the message will contain the names of the NVSCs 1211 that the entitlement agent wishes to have removed, and the name map in the EMM sent by the CAA will specify only the names of the NVSCs 1211 that the entitlement agent wishes to keep. It may, however, happen that the entitlement agent is not cooperative or that the conditional access authority must reduce the size of list 1411 for the entitlement agent before it receives a message from the entitlement agent. In that case, the CAA may remove NVSCs 1211 from list 1411 by the value of the name, beginning with the name with the highest numeric value, continuing with the next highest, and so on, until the required number of NVSCs 1211 have been removed.

The CAA can also use the Set EA Allocation Name Map EMM to remove EA information for an EA from DHCTSE 627. When the EMM is used in this fashion, none of the bits in the name map are set. CAA EMM code 1315 responds by returning all of the NVSCs in the EA information 1333 and EA Descriptor 1409(i) for the EA identified by the EAID in the EMM to free list 1407 and re-linking EA list 1406 as required.

Set EA Maximum Allocations

The Set EA Maximum Allocations EMM contains the EAID for the EA having the entitlement information 1333 that is being created or modified and also contains values for fields 1511 and 1515 of EAD 1409. CAA EMM code 1315 responds to this EMM by reading down EA list 1406 until it finds EA descriptor 1409 with the EAID specified in the EMM and then setting fields 1511 and 1515 of EAD 1409 using the values in the EMM. When an entitlement agent sends an EMM to DHCTSE 627 that establishes entitlement information of a certain type, for example, for an event, the code that interprets the EMM checks the EA maximum allocations to determine whether the maximum number of entitlements for that EA has been exceeded. In the preferred embodiment, entitlements are represented by NVSCs. Consequently, what is limited is the number of NVSCs of a given type in list 1411.

Update Entitlement Agent Public Key

The Update Entitlement Agent Public Key EMM contains the EAID for the EA having the entitlement information that is being created or modified and the EA's public key. CAA EMM code 1315 responds to this EMM by locating EA descriptor 1409 as described above and setting field 1527 from the public key in the EMM. With the EA's public key in place, DHCTSE 627 can then use the signed digests of the EMMs to verify that they are from the EA. This verification is possible since the EA uses the private key corresponding to the updated public key to perform the signing operation. EA EMMs that Modify Entitlement Information 1333

The EA EMMs that modify entitlement information have sealed digests that are encrypted using the EA's private key. The EMMs fall into two groups: EMMs that modify EA fields 1516 of EAD 1409 and EMMs that modify contents of the NVSCs making up list 1411. As set forth with regard to EAD 1409, each NVSC has a name, and each NVSC in list 1411 has a type. An NVSC is named by the CAA, as described above, and its name cannot be changed by the entitlement agent. The entitlement agent can, however, change the type and contents of a NVSC, subject only to the maximums for the types established in EAD 1409 for the EA. It is up to the entitlement agent to keep track of the types and contents of the NVSCs in EA information 1333.

The EMM that modifies EA fields 1516 of EAD 1409 is the Update Entitlement Agent Properties EMM. The second group of EMMs is further subdivided according to the kinds

of entitlements they provide. There are two broad families of entitlements: broadcast entitlements for non-interactive services and interactive entitlements for interactive sessions. Within the broadcast entitlements, there are further event entitlements for events that the user pays for individually, as is the case with pay-per-view events, interactive pay-per-view events, and near video-on-demand events. The non-event broadcast EMMs include:

- Update MSK
- Update Digital Bit Map
- Update Digital List
- Update Analog MSK and Bit Map
- Update Analog MSK and List
- Update Analog Bit Map
- Update Analog List
- The broadcast EMMs for events include
- New Event Storage
- Add/Remove PPV Event
- Acknowledge IPPV/NVOD Event
- The EMMs for interactive sessions include
- New Interactive Session Storage
- Add Interactive Session
- Remove Interactive Session

As can be seen from the names of the EMMs, the EA can change the type of the named NVSCs allocated by the CAA as needed for events and interactive sessions, subject only to the maximums specified in EAD 1409.

There are separate CAA EMMs for allocating NVSCs, setting limits on types of NVSCs, and assigning a public key to an entitlement agent. Also, the EA EMMs for writing NVSCs 1211 do so by name and can change the NVSC 1211 type as well as its content. Therefore, access control system 601 has a high degree of control and flexibility. A CAA may dynamically constrain the total number of entitlements that an entitlement agent may give, the types of entitlements, and the number of entitlements of each kind as required. The CAA may also change the constraints either in part or as a whole, and can do so either in cooperation with the entitlement agent or unilaterally. Within the constraints imposed by the CAA, however, the entitlement agent is free to dynamically manage its own entitlements, changing not only entitlements of a given type, but even changing the types themselves.

Update Entitlement Agent Properties

This EMM contains the values for EA fields 1516 of EAD 1409. EA administration EMM code 1317 reads EMM header 1113 to get the EAID for the EA to which the EMM is directed and simply sets fields 1516 in EAD 1409 for the EA from the EMM.

Non-Event Broadcast EMMs

Of the non-event broadcast EMMs, four types will be discussed here. These are Update MSK, Update Bit Map, Update List, and update combinations with MSK and list or bitmap. Those skilled in the art will be able to easily apply the principles explained below to EMMs that perform the functions indicated by the names of the other non-event broadcast EMMs. For example, the principles of digital EMMs can be applied to analog EMMs. There is a separate type of NVSC 1405 for each information type provided by the above non-event broadcast EMMs. FIG. 16 shows the contents of four of these types of NVSCs. Each NVSC type will be discussed together with the EMM that provides the information it contains.

Update MSK

The Update MSK EMM is used to send a new MSK for a set of services provided by the EA specified by the EMM.

The new MSK and other information associated with the MSK are stored in MSK NVSC 1601 in list 1411 for EA information 1333 belonging to the EA specified by the EMM. Included in MSK NVSC 1601 is header 1502. Header 1502 specifies that NVSC 1601 is a MSK NVSC, gives the NVSC's name, and contains next element pointer 1507 to the next element in list 1411. The other fields contain information about the MSK. In the preferred embodiment, MSK 1608 has two 128-bit parts: the even MSK 1609 and the odd MSK 1611. Each part has two halves, i.e., a first half and second half, each of which has 56 key bits and 8 unused parity bits. The MSK 1608 is associated with a pair identifier 1603 for MSK 1608, an expiration date 1605 for MSK 1608, and a flag 1607 indicating whether the value of expiration date 1605 should be ignored. If the expiration date 1605 is not to be ignored, DHCTSE 627 will not use MSK 1608 to decrypt a control word after the expiration date. The identifier 1603 is per-EA, and consequently, a given EA may have one or more MSK NVSCs 1601 at any given time to store a plurality of different MSKs. Thus, conditional access system 601 not only permits separate security partitions for each EA, but also permits security partitions within an EA.

The Update MSK EMM header contains the EAID needed to locate EA information 1333 for the EA; the message contains the name of the NVSC that is to receive the MSK, a MSK pair selector which specifies a MSK pair ID for the MSK to be updated, a set of flags permitting the EA to selectively change MSK pair ID 1603, expiration date 1605, no expiration date 1607 and either half of MSK 1608, and the information needed to make the changes. At a maximum, the EMM contains a value for MSK pair ID 1603, a value for expiration date 1605, a value for no expiration date 1607, and values for even MSK 1609 and odd MSK 1611. EA MSK code 1319 processes the Update MSK EMM by locating EA Information 1333 for the EA identified by the EMM header's EAID, using the cell name to locate the proper NVSC, giving that NVSC the MSK type, and then writing to the MSK NVSC 1601 as required by the flags and the information in the EMM. This procedure is the same for both analog and digital Update MSK EMMs. The differences are in the EMM command code in EMM Header 1123 and NVSC type 1503.

Entitlement Identifiers

As will be explained in more detail below, an ECM specifies the service instance that it accompanies by means of (1) the EAID for the entitlement agent that is the source of the ECM and (2) a 32-bit entitlement ID for the instance. Entitlement IDs are per-EA. By making the entitlement IDs 32 bits long, each EA will have enough entitlement IDs even for transient services such as pay-per-view events and interactive services. In the preferred embodiment, when DHCTSE 627 interprets an ECM, it checks whether DHCT 333 is entitled to decrypt the instance by looking in EA information 1333 for the EA specified in the ECM for an entitlement ID that corresponds to the entitlement ID specified in the ECM. The entitlement IDs in the EMM and in EA information 1333 can be represented in at least two ways. One way is by simply listing entitlement IDs. The drawback with this technique is that the 32-bit entitlement IDs are large, and NVSCs are a scarce resource. The other way is by means of a starting entitlement ID value and a bit map. Any entitlement ID having a value within 255 of the entitlement ID value specified by the starting entitlement ID value can be specified by setting a bit in the bit map. This technique is set forth in the Banker and Akins patent application supra. See particularly FIG. 2 of the Banker and Akins patent application and the discussion of that figure. The following

discussion of specifying entitlement IDs by means of a starting ID and a bit map is an expansion of the discussion in that patent application.

Update Bit Map EMM

This EMM updates a bit map that specifies one or more entitlement IDs. The bit map is stored in an entitlement bit map NVSC 1613. NVSC 1613 has a header 1502 with the cell number and type of the NVSC; a first entitlement ID 1615, which is the first entitlement ID which may be specified by the bit map; an expiration date 1617, which specifies when the entitlement IDs specified by first entitlement ID 1615 and the bit map expire; a no expiration date flag 1619, which indicates whether there is in fact an expiration date; and bit map 1621. The update bitmap EMM contains the cell name for the NVSC 1613 to be set, a set of flags which indicate the information in NVSC 1613 that is to be set by the EMM, and the values for the information. The EMM may set any or all of first entitlement ID 1615, expiration date 1617, no expiration date 1619, and bit map 1621. EA administrative EMM code 1317 responds to the EMM by setting the fields of the specified NVSC 1613 as indicated in the EMM. This procedure is the same for both Update Digital Bit Map and Update Analog Bit Map EMMs. The differences are in the EMM command code in EMM Header 1123 and NVSC type 1503.

Update List EMM

The Update List EMM updates a list of entitlement IDs that is contained in an entitlement list NVSC 1623. NVSC 1623 has a header 1502 with the cell name and type for the NVSC and contains up to six entitlement ID elements 1625. Each of the elements contains an entitlement ID 1627, an expiration date 1629 for the entitlement ID, and a flag 1631 indicating whether the entitlement ID has an expiration date. The update list EMM contains the cell name for the NVSC, a value for the flag, an expiration date, and values for up to six entitlement ID elements 1625. This procedure is the same for both Update Digital List and Update Analog List EMMs. The differences are in the EMM command code in EMM Header 1123 and NVSC type 1503.

Broadcast Events

A broadcast event is a one-time service, such as a pay-per-view broadcast of a boxing match. In the preferred embodiment, there are two kinds of broadcast events: ordinary pay-per-view broadcast events, in which the customer has ordered in advance to see the event, and impulse events where the customer decides at the time the event is broadcast that he wants to order it. There are different kinds of impulse events, such as: impulse pay-per-view (IPPV) events, which are pay-per-view events where the customer can decide at the time of the event to purchase it, and near video-on-demand (NVOD), where popular movies are rebroadcast at short intervals and the customer can decide when the rebroadcast occurs whether he or she wants to view it. Those skilled in the art will realize that the concept of an "event" can refer to any service over a specific time period (whether broadcast or non-broadcast), such as video on demand events or other types of events not listed here.

In the case of pay-per-view events, the customer orders the event from the entitlement agent, and the agent responds by sending an EMM that contains the necessary entitlement information. In the case of events where the customer decides at broadcast time that he or she wants to purchase the event, purchase information, i.e., information about the entitlements that can be purchased, must be distributed with the event. In these cases, the purchase information is distributed by means of global broadcast authenticated messages, or GBAMs. The customer provides input 628 that

specifies a purchase. The DHCT 333 responds to the input 628 by storing the record of purchase in the DHCTSE 627 and then beginning to decrypt the event. Later, the DHCT 333 sends the entitlement agent a forwarded purchase message (FPM) indicating what has been purchased by the customer, and the entitlement authority responds with an EMM that confirms the purchase and contains the necessary entitlement information. The record of the purchase remains until an EMM confirming the purchase is received by the DHCTSE 627.

Event NVSCs: FIG. 17

FIG. 17 shows event NVSC 1701 used to store entitlement information for events. Header field 1502 is similar to that for other NVSCs 1701. Each event NVSC 1702 may contain up to three event descriptors 1703, each of which describes a single event. Each event descriptor 1703 contains a Flags Field 1705 that includes flags to indicate (1) whether the event is active, (2) whether its end time has been extended, (3) whether the entitlement agent has confirmed purchase of the event, (4) whether the customer can cancel at any time, (5) whether the customer can cancel in a cancellation window, (6) whether the customer has canceled the purchase, (7) whether the right to copy the event has been purchased, and (8) whether the event is an analog or digital service. Purchase time 1709 is the later of the start time for the event or the time the customer purchased the event. End time 1709 is the time the event is to end. Cost 1711 is the cost of the event to the customer, and entitlement ID 1713 is the entitlement ID for the event.

New Event Storage EMM

When the CAA sets up entitlement agent descriptor 1409 for an entitlement agent, it includes a value in EA Maximums 1515 that limits the number of event NVSCs 1701 the entitlement agent may have. Within that number, however, the entitlement agent is free to allocate event NVSCs 1701 from the total number of NVSCs 1405 belonging to the entitlement agent and to reuse existing event NVSCs 1701. To allocate an event NVSC, the EA uses the new event storage EMM, which simply contains the cell name for the NVSC which is to be allocated. Once the event NVSC 1701 has been allocated, its fields are set as follows:

In the case of an ordinary PPV event, fields are set by an add/delete event EMM;

In the case of an IPPV or NVOD event, fields are set in part from the GBAM for the event and in part from customer input 628.

The contents of an event NVSC 1701 are deleted by an add/delete event EMM or by receiving an ECM containing a time greater than the event end time in the event NVSC 1701, if the event record had been previously acknowledged by receiving the Acknowledge Event EMM.

The Add/delete Event EMM

The add/delete event EMM contains a flag which indicates whether the EMM is setting or deleting an event. In the latter case, the contents of the EMM must match the current contents of the NVSC 1701 that is to be deleted. In the former case, the values of the EMM include flags indicating whether time extensions are allowed and whether the right to copy has been purchased. Further included are values for the event's start time and end time and the entitlement ID for the event. When the add/delete flag indicates "delete", EA administrative code deletes the contents of the NVSC 1701. When it indicates "add", the code sets the corresponding fields of the NVSC 1701 to the values specified in the EMM. The flag that indicates whether the EA has acknowledged the purchase is set to so indicate.

The Global Broadcast Authenticated Message: FIGS. 18-20

The Global Broadcast Authenticated Message (GBAM) is, like the EMMs, ECMs, and FPMs, a CA message. A GBAM is broadcast by an entitlement agent to DHCTs 333. FIG. 18 shows a CA message 805 including a GBAM 1801. Message 805 includes a CA message header 1003 and a CA GBAM message 1803, which in turn is made up of a GBAM header 1807 and global broadcast data 1809. Global broadcast data 1809 is not encrypted, but GBAM 1801 is authenticated in the same fashion as an ECM: header 1807, global broadcast data 1809, and MSK 1015 belonging to the EA which sent the GBAM are hashed by one-way hash function MD5 to produce GBAM MAC 1805. As with the ECM, the MSK 1015 is a shared secret between the EA which sent the GBAM and DHCTs 333 that have EA information 1333 for the EA.

FIG. 19 shows GBAM header 1807 in detail as well as the form that global broadcast data 1809 takes when GBAM 1801 is used to provide entitlement information for IPPV or NVOD. GBAM header 1807 has a conditional access system ID 1901 that identifies CA system 601 in which GBAM 1801 is being used, a tag which indicates that the message is a GBAM, and the identifier 1905 of the entitlement agent sending the GBAM. Fields 1907 and 1909 specify the key that was used to make MAC 1805. Field 1907 specifies the parity of the MSK half used to make the digest, and MSK select 1911 is an identifier for the MSK itself.

Purchasable entitlement data 1913 refers to the form of global broadcast data 1809 that is used to provide entitlement information for IPPV or NVOD. Of the fields that are relevant for the present discussion Entitlement ID 1915 is the entitlement ID for the event associated with the GBAM, and Flags 1917 include flags indicating what kind of cancellation is allowed and whether the time for the event may be extended. Number of modes 1919 indicates how many different modes there are for purchasing the event. The rights which the purchaser receives to the event and the price the purchaser must pay will vary with the mode. In the preferred embodiment, an event may have up to five purchase modes. If more purchase modes are required, additional GBAMs may be sent. The rights and prices for each mode are indicated by arrays. Each array has as many valid elements as there are modes. The value of an element corresponding to a mode indicates the right or price for that mode. Thus, mode right to copy field 1921 is a bit array; if a bit for a mode is set, the purchaser of the mode has the right to copy the event. Similarly, mode length field 1927 contains a value for each mode which indicates the length of time for the event in that mode. Mode cost field 1929 contains a value for each mode which indicates the cost for the event in that mode. Earliest start field 1923 gives the earliest time at which entitlement for the event can start, and latest end field 1925 gives the latest time at which entitlement must end.

When DHCT 333 receives GBAM 1801, it passes GBAM 1801 to DHCTSE 627 for authentication of global broadcast data 1809. Authentication will fail unless DHCTSE 627 has the required MSK. If (1) DHCTSE 627 has the required MSK and (2) global broadcast data 1809 is data 1913, DHCT 333 permits the customer to purchase the event. In so doing the customer identifies himself or herself to DHCT 333 by means of a PIN, and that PIN must match PIN 1525 in EAD 1409 for the entitlement agent that sent the GBAM. In making his or her purchase, the customer also specifies the relevant modes. Given the mode information and the cost information in the GBAM, DHCT 333 can determine whether ordering the impulse event will cause the customer to exceed the amount (of time, money, etc.) specified in

stored credit limit 1519 in EAD 1409. If the customer has not exceeded the limit, the information from the GBAM and from the purchaser's inputs are used to make an event descriptor 1703 for the event. DHCT 333 passes the information to DHCTSE 627, which sets the fields in event descriptor 1703 according to the values provided it by DHCT 333. The flag that indicates whether the purchase information has been acknowledged is cleared, and the cost of the event is added to the current credit balance.

The Forwarded Purchase Message: FIG. 21

The forwarded purchase message (FPM) in a preferred embodiment serves two purposes:

- it informs the entitlement agent that the customer has purchased an IPPV or NVOD event; and
- it informs the entitlement agent that the customer has canceled the purchase of any event.

In other embodiments, messages like the FPM can be used to transfer any kind of information from DHCT 333 to a CAA or an EA. For example, such a message can be used to transfer monthly order information from DHCT 333 to an EA.

DHCT 333 sends a forwarded purchase message with the purchase information via the reverse channel to the entitlement agent that sent the GBAM. The FPM is contained in a reverse channel data packet that is addressed to the EA. FIG. 21 provides an overview of the FPM and of the cryptographic measures used to protect its contents. FPM 2101 is a CA message 805 and consequently is sent with a CA message header 1003. FPM 2101 itself is made up of FPM encrypted envelope key 2103, which contains the EAID for the entitlement agent and FPM key 2119 for decrypting the purchasing information contained in FPM encrypted events 2113. The key and other contents of envelope key 2103 are encrypted for privacy using the public key of the entitlement agent for which FPM 2101 is intended. CA FPM message 2105 includes CA FPM header 211, which includes the EAID for the intended EA, and FPM encrypted events 2113. The latter are encrypted using the 3-DES algorithm with the key in envelope key 2103. CA FPM message 2105's parts are a header 213, FPM clear events 2133, which contains the purchase information, and padding 2135. The last part of FPM 2101 is FPM signed authentication 2107, which is encrypted with the private key of DHCT 333 from which FPM message 2101 is sent.

The encrypted material includes FPM signing header 2125, FPM MAC 2127, and padding 2129. FPM MAC 2127 is made using the MD 5 one-way hash algorithm from FPM clear events 2133. Only the EA for which the FPM is intended can decrypt envelope key 2103 to obtain key 2119 to decrypt FPM encrypted events 2123, and the EA can check the authenticity of FPM clear events 2133 only if it has the public key for DHCT 333 from which FPM 2101 was sent.

The part of FPM 2101 which is of further interest here is FPM clear events 2133. The information in that part of the FPM includes the serial number of DHCTSE 627 in DHCT 333 from which the message came, the EAID of the destination EA, and an indication of the number of events for which the FPM contains purchase information. The information for each event is contained in forwarded event data for that event. The forwarded event data is taken from GBAM 1801 and event descriptor 1703 for the event. Fields of interest in the present context include flags indicating (1) whether the event has been extended, (2) whether the user has canceled the event, and (3) whether the customer has purchased the right to copy. Other information includes the time the event started or was purchased, whichever is later,

the time the event is to end, its cost to the customer, and the entitlement ID for the event. To cancel any event, including an ordinary pay-per-view event, DHCT 333 sends an FPM with the same message, but with the event canceled flag set to indicate cancellation. The conditions under which DHCT 333 sends an FPM cancellation message will be explained in more detail below. FPMs may also be used to purchase other service types, such as monthly subscriptions, or data downloads, for example.

The Acknowledge IPPV/NVOD Event EMM

When the entitlement agent receives the FPM, it enters the information contained in the FPM in its customer information database and returns an acknowledge IPPV/NVOD event EMM to DHCT 333. EMM command data 1125 in this EMM contains an exact copy of the forwarded event data in the FPM that the EMM is acknowledging. When DHCTSE 627 receives this EMM, it decrypts and authenticates it and then, for each item of copied forwarded event data, it uses the entitlement ID to locate event NVSC 1701 for the event. Having located the event NVSC 1701, it compares the copied forwarded event data with the corresponding fields of event NVSC 1701. If they are the same, DHCTSE 627 sets the flag in Flags Field 1705 that indicates that the purchase has been confirmed and adjusts the stored credit balance. If the EMM has its "canceled" flag set, the "in use" flag in event NVSC 1701 is set to indicate that event NVSC 1701 is not in use and is therefore available for reuse by the entitlement agent.

Other uses of GBAM 1801

GBAM 1801 can be used generally to broadcast authenticated messages via a MPEG-2 transport stream, or other transport mechanisms, to DHCTs 333. CA system 601 itself uses GBAM 1801 in two other ways: to periodically broadcast a time value to DHCTs 333 and to extend the time for events. In the former case, GBAM 1801 simply carries the time value, which is a secure time, due to the GBAM's authentication. The code in DHCT 333 which carries out a task for the entitlement agent that sent the system time GBAM can use the time value to coordinate its activities with activities by the EA. Note that this arrangement permits the use of per-entitlement agent time schemes. It also permits establishing a uniform system time throughout a digital broadband delivery system by setting up one entitlement agent in each DHCT 333 of the digital broadband delivery system as the "system time entitlement agent" and addressing the system time GBAM to the system time entitlement agent.

GBAMs 1801 that extend the time for an event carry the entitlement ID for the event and the number of minutes the time for the event is to be extended. When GBAM 1801 is received and provided to DHCTSE 627, the secure element adds the number of minutes to end time 1709.

FIG. 20 shows a server application 2001 executing on a processor having access to entitlement agent 2005 and to the MPEG-2 transport stream being received by a group of DHCTs 333. The server application 2001 can use GBAM 1801 to send authenticated messages to the DHCTs 333. Server application 2001 sends a message to entitlement agent 2005, which uses its transaction encryption device 603 to make a GBAM 1801 including the payload. Entitlement agent 2005 then returns the GBAM to server application 2001 which sends application data together with the GBAM, as shown at 2007, to client application 2009 in the DHCTs 333. Each client application sends GBAM 1801 to DHCTSE 627, which authenticates it. If the authentication succeeds, DHCTSE 627 sends an acknowledgment to client application 2009. It should be noted here that it is the entitlement agent and not server application 2001 which authenticates the payload.

NVSCs and EMMs for Interactive Sessions

DBDS 501 can also be used for interactive sessions. Examples of such uses are browsing the Internet or playing video games. In such applications, data being sent to the customer will generally go via the MPEG-2 transport stream, while data being sent from the customer will go via the reverse channel. Such an arrangement is advantageous for the many interactive applications in which the customer receives a large amount of data, for example, the data that represents an image, makes a short response, and then receives another large amount of data.

Each interactive session that is currently taking place with a user of DHCT 333 has an interactive session NVSC 1211 in list 1411 belonging to the entitlement agent that grants access to the interactive session. The interactive session NVSC contains a session key for the interactive session and an entitlement ID for the interactive session. DHCTSE 627 allocates the interactive session NVSC in response to a new interactive session storage EMM from the entitlement agent. The new interactive session storage EMM simply contains the cell name of the NVSC to be used for the interactive session.

Once the EA has established the NVSC, it sends an "add interactive session" EMM that is directed to the name of the newly-allocated NVSC and contains the entitlement ID and the key for the interactive session. The secure element places the entitlement ID and key in the NVSC. When the EA determines that the interactive session is over, it sends a "remove interactive session" EMM with the entitlement ID for the interactive session and the secure element deletes the contents of the NVSC. It is of course possible that the entitlement agent sends a new interactive storage EMM at a time when all of the interactive session NVSCs allotted by the CAA to the EA are already in use. DHCTSE 627 in a preferred embodiment deals with this situation by keeping track of the last time each interactive session sent or received data. When a new interactive session is needed and none is available, DHCTSE 627 shuts down the interactive session that least recently sent or received data and uses that interactive session's interactive session NVSC for the new interactive session. Another solution is to request the user to select an interactive session to be terminated.

Details of the ECM: FIG. 22

The information in an ECM that is used to determine whether the instance of a service that the ECM accompanies is to be decrypted in a given DHCT 333 is contained in ECM entitlement unit message 1011. FIG. 22 gives details of the contents of ECM entitlement unit message 1011 for a preferred embodiment of the present invention. Beginning with message ID 2205, the two fields 2201 and 2203 identify this message as an ECM entitlement unit message. EAID 2207 is the identifier for the entitlement agent which grants entitlements to access to the instance of the service that the ECM accompanies.

Decryption information 2209 is information used to produce the control word 2235. Control word counter value 2235 is encrypted using the 3DES algorithm in a preferred embodiment. This algorithm employs two keys, and in a preferred embodiment, each key is $\frac{1}{2}$ of the MSK. Also, there are two versions of the MSK: even and odd. MSK parity 2211 specifies which version is to be used in the 3DES algorithm. MSK ID 2213 specifies which MSK belonging to the entitlement agent is to be used, or if the ECM accompanies data for an interactive session, it specifies that the key is to be found in the NVSC for the interactive session. Control word parity 2215 specifies the parity of the unencrypted control word 2235. Parity count 2217 is a 0-1

counter that has the value 0 when the parity of the control word is even and 1 when it is odd.

Free preview 2219 is a flag that indicates that the ECM is accompanying a portion of the service instance that is a free preview. That is, as long as a customer has the MSK for decrypting the service instance, the customer needs no further entitlements to view the free preview portion of the service. The main use of free previews is with IPPV or NVOD services. Copy protection level 2221 is a value which indicates to what extent the instance may be copied. Blackout/spotlight 2223 is a value which indicates how blackout/spotlight information 2236 is to be used: not at all, for a blackout, or for a spotlight (i.e., the service is targeted to the specific area).

Number of entitlement IDs 2225 specifies the number of entitlement IDs 2245 that are contained in this ECM. The maximum number in a preferred embodiment is six in a single ECM. Multiple ECMs may be sent for each service. Allow IPPV 2229 is a flag which indicates whether the service instance may be viewed on an IPPV or NVOD basis. Cancel window 2231 is a bit that is set in a service instance that may be viewed as an event to indicate the end of the period during which the customer may cancel the event. Time stamp 2233 is a time stamp indicating the time at which the ECM was created. Encrypted control word 2235 is the control word contained in the ECM. It is encrypted using the 3DES algorithm and the MSK for the service instance.

Blackout/spotlight information 2236 defines a geographic area which is to be blacked out or spotlighted by an instance of a service. It does so by means of x centroid 2239 and y centroid 2241, the two of which define a point in a geographical coordinate system defined by the entitlement agent, and blackout radius 2237, which is used to determine a square that is centered on the point defined by fields 2239 and 2241 and that has sides that are twice the value of blackout radius 2237. Entitlement ID list 2243 contains from one to six entitlement IDs for the instance of the service that the ECM accompanies.

Details of Blackout/spotlight Info 2236: FIGS. 26 and 27

The coordinate system used in a preferred embodiment is shown in FIG. 26. Coordinate system 2601 is a 256 unit by 256 unit square, with the origin at the lower left-hand corner. In the coordinate system, it is the lines, rather than the spaces between them, that are numbered. The entitlement agent to which coordinate system 2601 belongs assigns each DHCT 333 in the area covered by the coordinate system the coordinates of an intersection of a line that is perpendicular to the x axis with a line that is perpendicular to the y axis. Thus, a DHCT 333(k) may be assigned the point (i,j) 2603 in coordinate system 2601.

FIG. 27 shows how areas are defined in coordinate system 2601. Area 2705 has its centroid 2701 at the point whose coordinates are (57,90). The radius 2703 of the area is three, so this number is added to and subtracted from each of the coordinates of the centroid to produce a square 2705 whose lower left-hand corner is at (54,87) and whose upper right-hand corner is at (60,93). In the preferred embodiment, points on the left and bottom lines are in the area; points on the top and right lines are not.

Determining whether to Decrypt the Service Instance that Accompanies an ECM

Conceptually, what happens when DHCT 333 receives an ECM accompanying an instance of a service is that DHCT 333 provides the ECM to DHCTSE 627, which examines the NVSCs in EA storage 1331 to find whether the customer to whom DHCT 333 belongs is entitled to receive the instance

Entitlement
IDs

of the service. If the customer is so entitled, DHCTSE 627 decrypts the control word in the ECM and provides it to service decryptor 625, which uses it to decrypt the MPEG-2 packets containing the audio and video for the service. However, the number of different kinds of services, the number of different ways in which a service can be purchased, and the number of ways in which access can be restricted all work together to make the manner in which DHCTSE 627 processes an ECM rather complex.

The simplest case is for a broadcast service such as a standard CATV channel. Here, the customer who owns DHCT 333 has paid his or her monthly bill for the service and the entitlement authority has sent two EMMs to DHCT 333: a MSK EMM with the month's MSK for the service and an EMM that specifies the entitlement ID for the service. As previously pointed out, the latter EMM may either contain a list of entitlement IDs or a first entitlement ID and a bit map. All of these EMMs may also contain expiration dates: in the case of the MSK EMM, there is an expiration date of the MSK; in the case of the entitlement ID list EMM, there is an expiration date for each entitlement ID on the list; in the case of the entitlement bit map EMM, there is an expiration date for the entire bit map.

At a minimum, EA information 1333 for the entitlement agent that provides entitlements for the service instance that the ECM is accompanying contains EA descriptor 1409, a MSK NVSC 1601, and either an entitlement bit map NVSC 1613 or an entitlement list NVSC 1623 for the service to which the instance belongs. EA information 1333 may also contain NVSCs with entitlement information for many other services or instances thereof.

The ECM for the service instance will contain, at a minimum, entitlement agent ID 2207, decryption information 2209, time stamp 2233, encrypted control word 2235, and a single entitlement ID 2245 for the instance of the service.

When DHCT 333 receives the ECM, it delivers the ECM to DHCTSE 627, which reads down EA list 1406 until it finds an EA descriptor 1409 having a value in EAID 1509 that is the same as the value EAID 2207 in the ECM. DHCTSE 627 then follows first NVSC pointer 1513 to list 1411 and looks for a MSK NVSC 1601 that has an MSK ID field 1603 containing the same value as MSK ID field 2213 in the ECM. Having found such an MSK NVSC, it determines from no_exp_dat flag 1607 whether expiration date field 1605 contains a valid time value, and if so, it compares that value with the value in the ECM's time stamp field 2233. If the value in time stamp field 2233 is more recent in time, DHCTSE 627 will not use MSK 1608 from MSK NVSC 1601 to decrypt control word 2235. The secure element continues searching for an MSK NVSC with the proper MSK ID and an unexpired MSK, and if it finds such a MSK NVSC, it uses that MSK NVSC; if it finds no such MSK NVSC, it does not decrypt the control word.

DHCTSE 627 similarly searches list 1411 for an entitlement bitmap NVSC 1613 or an entitlement list NVSC 1623 which contains an entitlement ID which is the same as one of the entitlement IDs 2245 in the ECM. If (1) DHCTSE 627 finds an NVSC with such an entitlement ID and (2) there is no valid expiration time in the NVSC that specifies the entitlement ID that is earlier than time stamp 2233 in the ECM and (3) DHCTSE 627 has also found a valid MSK NVSC 1601 as described above, DHCTSE 627 decrypts control word 2235 using the MSK and decryption information 2209 in the ECM. Decryption is done using the 3DES algorithm that was used to encrypt the control word. In a preferred embodiment, the control word contained in the

ECM is a counter value as described above, and DHCTSE 627 produces the control word that actually is used to decrypt the service instance by re-encrypting the integer using the MSK and the 3DES algorithm. That control word usable by the service decryptor is then returned to service decryption module 625, which uses it to decrypt the service instance.

As is apparent from the foregoing description when DHCTSE 627 searches an entitlement agent's entitlement agent information 1333 for a given entitlement for a service, it continues searching until it has either found an NVSC that contains the entitlement or it has reached the end of list 1411. What this means in logical terms is that the entitlements that a given entitlement agent can grant are the logical OR of the entitlements specified in entitlement agent information 1333. For example, if one entitlement bit map NVSC that contains the same entitlement ID as the ECM has expired but another has not, DHCTSE 627 disregards the expired NVSC, and based on the active NVSC, produces control word 2235.

It should further be pointed out here that time stamp 2233 in the ECM and the expiration information in the NVSCs prevent reuse of a previous month's MSK to decrypt an instance in the current month and also prevent reuse of a previous month's entitlements in the current month to implement the protection against replay attacks described in the Banker and Akins patent application supra.

Where further restrictions apply to an entitlement, DHCTSE 627 searches for that information as well in entitlement agent information 1333. For example, if blackout/spotlight field 2223 of the ECM indicates that a blackout applies to the service, DHCTSE 627 uses blackout/spotlight information 2236 to determine whether the location specified by x coordinate 1521 and y coordinate 1523 is within the square specified by blackout/spotlight information 2236; if so, DHCTSE 627 does not decrypt control word 2235. When a spotlight applies, the procedure is of course the opposite: DHCTSE 627 decrypts the control word only if x coordinate field 1521 and y coordinate field 1523 specify a location within the square.

As previously noted, the techniques that are used to grant entitlements according to geographical area may be generalized to grant entitlements to various subsets of customers. For example, entitlements may be conceptually represented in a Venn diagram, blackout/spotlight information 2236 may specify an area in the Venn diagram that represents the set of customers that are entitled to receive the service, and x coordinate 1521 and y coordinate 1523 may specify the location of the customer in the Venn diagram. One use of such an arrangement would be to restrict access to an instance of a service according to a customer's desire that users of his or her DHCT not have access to instances with objectionable content. In other embodiments, of course, more coordinates or other ways of representing set membership could be used.

Event Services

When the ECM accompanies an instance of an event, interpretation of the ECM takes place as described above, except that the entitlement information for the event is contained in an event NVSC 1701. DHCTSE 627 searches the entitlement information 1333 for the entitlement agent having the EAID that is in the ECM for an event NVSC 1701 containing an event descriptor 1703 with an entitlement ID 1713 that is the same as one of the entitlement IDs 2245 in the ECM. If the event is a standard pay-per-view event, DHCTSE 627 then examines the flags 1705 to determine whether the customer has canceled the event and whether

purchase of the event has been confirmed (always the case with standard pay-per-view). The DHCTSE 627 then compares purchase time 1707 and end time 1709 with time stamp 2233 to determine whether the time indicated by the time stamp is within the period indicated by fields 1707 and 1709. If the examination of event NVSC 1701 indicates that the customer is entitled to the event, DHCTSE 627 decrypts control word 2235 as described above.

With IPPV or NVOD events, allow IPPV flag 2229 in the ECM must indicate that the event is one that need not be purchased in advance. Free preview flag 2219 may also be set to indicate that the portion of the event instance accompanied by the ECM is part of the free preview, and cancel window flag 2231 may further be set to indicate that the event can still be canceled. If free preview flag 2219 is set, DHCTSE 627 simply looks for a MSK NVSC 1601 in EA information 1333 that contains the MSK specified by MSK ID 2213 in the ECM. If the DHCTSE 627 finds one that is valid, it decrypts control word 2235.

If free preview flag 2219 is not set, DHCTSE 627 goes to the event NVSC 1701 having the entitlement ID 1713 that is the same as one in ECM field 2245. If flags included in flags 1705 indicate that the purchase of the event has been confirmed and the event has not been canceled, DHCTSE 627 decrypts control word 2235. If the event has not been canceled and has not been confirmed, but time stamp 2233 indicates a time that is within a predetermined period after purchase time 1707 indicated in event descriptor 1703, DHCTSE 627 also decrypts control word 2235. It is by this means that the service instance continues to be decrypted between the time the FPM is sent to the entitlement agent and the time the entitlement agent returns the acknowledge IPPV/NVOD event EMM. This causes the confirmation flag to be set in flags 1705.

Cancellation of Entitlements to Events: FIGS. 17, 19, and 22

Whether a user can cancel a previously purchased entitlement to an IPPV/NVOD event that he or she has purchased preferably depends on the event. There are three possibilities:

- the entitlement can be canceled up to two minutes past purchase;
- the event can be canceled during a period of time termed a cancellation window; or
- the event cannot be canceled.

Which of the three possibilities is associated with a given event is determined by the purchasable entitlement data 1913 in the GBAM that accompanies the event. One flag in flags 1917 indicates whether the event can be canceled; another indicates whether cancellation is possible in a cancellation window. If neither flag is set, the event cannot be canceled. When DHCTSE 627 makes an event descriptor 1703 for the event, the values of the flags in the GBAM are used to set flags in flags 1705 which indicate whether the event may be canceled or during a cancellation window only. Again, if neither flag is set, the event cannot be canceled.

The user cancels an event by requesting cancellation via customer input 628 to DHCT 333. When DHCT 333 receives the input, it provides a cancellation request, including the EAID and entitlement ID for the instance, to DHCTSE 627, which uses the EAID and the entitlement ID to locate the event NVSC 1701 that contains event descriptor 1703 for the event. If the flags in flags 1705 indicate that the entitlement cannot be canceled, DHCTSE 627 indicates that fact to DHCT 333, which then indicates that the entitlement is not cancelable to the user. If the flags indicate that the entitlement can be canceled, DHCTSE 627 simply

sets the canceled flag in event descriptor 1703. If the flags indicate that the entitlement can be canceled only during a cancellation window, and an ECM indicating the cancel window has ended has not yet been received, DHCTSE 627 sets the cancel flag in event descriptor 1703; otherwise, it indicates to DHCT 333 that the entitlement cannot be canceled, and DHCT 333 so informs the user. If the event has been canceled, DHCTSE 627 clears the acknowledged flag, which action causes a new FPM to be sent to the entitlement agent for the event. The entitlement agent responds to the FPM by adjusting its billing as required by the cancellation and sending a new acknowledge EMM.

Interactive Sessions

The chief difference between broadcast services and interactive services is that each session of the interactive service has its own interactive session key, which is contained in the interactive session NVSC for the interactive session. The NVSC for the interactive session also contains the entitlement ID for the interactive session. In an ECM that accompanies the MPFG-2 stream for an interactive session, MSK ID field 2213 is set to a value which indicates that the MPEG-2 stream is to be decrypted using an interactive session key. When DHCTSE 627 interprets such an ECM, it uses entitlement ID 2245 to find the NVSC for the interactive session and then uses the interactive session key contained in the NVSC to decrypt control word 2235.

Detailed Description of Transaction Encryption Device 603: FIGS. 24 and 25

Each CAA that can authorize entitlement agents in digital broadband delivery system 501 and each EA that can grant entitlements in system 501 has a Transaction Encryption Device or TED 603 in system 501. Preferably, each CAA or EA has its own separate TED in system 601. Alternatively, the TEDs could be combined in one device. The TED 603 stores the secret keys used by the entity to which it belongs and has hardware and software to do encryption, decryption, key generation, and authentication as required by the entity. The keys are kept secure by implementing the TED without a user interface or user I/O devices, by implementing it in a tamper resistant container, by connecting the TED only to the DNCS and using a secure link for that connection, and by keeping the TED in a physically secure environment such as a locked room.

In the case of a TED 603 for a CAA, the TED 603 stores the private keys corresponding to the three public keys representing the CAA in the DHCTs 333, encrypts and provides sealed digests for of EMMs from the CAA to the DHCTs 333, and decrypts and authenticates messages from the DHCTs 333 to the CAA. In the case of a TED 603 for an EA, the EA TED does the following:

- (1) stores the public and private keys for the EA and the MSKs for the EA;
- (2) generates the EA public and private keys and the MSKs;
- (3) encrypts and prepares sealed digests for the EMMs sent on behalf of the EA;
- (4) prepares the shared secret digests used to authenticate global broadcast messages;
- (5) provides the MSKs to SEES module 620 for use in encrypting instances of services;
- (6) generates interactive session keys (ISKs) for interactive session EMMs and provides them to SEES module 620 for use in encrypting the interactive session; and
- (7) decrypts FPMs and other messages sent from DHCT 333 to the entitlement agent.

TED 603 in Conditional Access System 601: FIG. 24

FIG. 24 shows the relationship between a number of TEDs 603 and the rest of conditional access system 601. Portion 2401 of conditional access system 601 includes a CAA TED 2427 for a CAA that authorizes entitlement agents in system 601. Portion 2401 also includes one EA TED 2425 for each of the n+1 entitlement agents which the CAA has currently authorized for DHCTs 333 in digital broadband delivery system 501. Alternatively, all EA TED 2425 functions could be combined into a single TED, which could include the CAA TED 2427 function. Each TED is kept in a physically secure area 2428 and is connected to DNCS 507 by a secure high-speed link 2423 that connects only DNCS 507 and the TEDs 603. In the preferred embodiment, the secure link is a secure Ethernet link. DNCS 507 uses TED 605 to encrypt EMMs, to decrypt FPMs, to generate EA public and private keys, to generate MSKs and ISKs, and to prepare global broadcast message digests. DNCS 507 has a remote procedure call interface to the TEDs 603 for performing these operations, and, consequently, programs executing on DNCS 507 can use the facilities of a TED simply by making a procedure call.

DNCS 507 is the sole connection between a given TED 603 and the rest of conditional access system 601. DNCS 507 is connected by a network 2415 to systems belonging to the CAA and the various EAs. Each of these entities has a database containing information relative to its function. CAA 2405 has CAA database 2403, which contains at least the CAA's three public keys and encrypted versions of the corresponding three private keys, the entitlement agent identifiers for the entitlement agents that the CAA authorizes, and a per-DHCT database that contains the names, types, and numbers of the NVSCs that the CAA has allocated to each entitlement agent authorized for the DHCT.

Each EA 2409(i) has its own EA database 2407(i). EA database 2407(i) preferably contains the EAID for the EA, a list of the MSK IDs and expiration dates for the MSKs that the EA is currently using, and a database of the services and/or instances that the EA is providing. This database of services contains at least the entitlement ID for each service. EA database 2407(i) also includes a per-DHCT database of the entitlement IDs, entitlement expiration times, and MSK IDs for the entitlements and MSKs sent in EMMs to the DHCT. The per-DHCT database may also contain customer billing information such as the information required to deal with the purchase information in an FPM.

Key certification authority 2413 is an entity which certifies the public keys of DHCTs 333 to DNCS 507. In a preferred embodiment, key certification authority 2413 is maintained by the manufacturer of DHCTs 333. DHCT key database 2411 contains a database of DHCT serial numbers and their public keys. When a user of a DHCT 333 wishes to purchase an instance of a service offered by an EA, the user sends a purchase order to the EA with the serial number (which is also the IP address) of the DHCT 333. The EA provides the serial number to DNCS 507, which maintains a database 2421 of DHCT public keys by serial number. If the serial number is not in the database, DNCS 507 sends a request for the public key to KCA 2413. The request contains the serial number, and the key certification authority responds to the request by sending a digitally signed message 2412 to DNCS 507. This message contains the DHCT's public key. DNCS 507 has the public key for the key certification authority and uses the public key and the digital signature to confirm the authenticity of the DHCT public key in the message. If the public key is authentic, DNCS 507 places it in public key database 2421.

DNCS 507 is further connected via another high-speed link 2417 to SEES 620, which is provided with MSKs for encrypting instances of services. Additionally, DNCS 507 provides global broadcast messages (GBAMs) and EMMs for broadcast via transport link 517 to the DHCTs 333. Finally, DNCS 507 is connected via the reverse path provided by LAN interconnect device 617 to the DHCTs 333 and receives FPMs from the DHCTs 333. In other embodiments, DHCT 333 may also send EMMs to DHCTs 333 by this route.

Data flows in portion 2401 are shown by labels on the arrows connecting the components. Thus, an EA 2408(i) sends unencrypted contents 2410 of EA EMMs and global broadcast messages to DNCS 507 and receives unencrypted contents 2412 of FPMs for the EA from DNCS 507. With EA EMMs and global broadcast messages, DNCS 507 uses EA TED 2425(i) to do the necessary encryption, digest making, and key generation and then sends the encrypted and authenticated EMMs and global broadcast messages, as well as the MSKs, to SEES 620, as shown at 2426 and 2418. In the case of EMMs, which are repeatedly sent over an extended period of time to the DHCTs, DNCS 507 stores the encrypted EMMs in EMM database 2420 and provides them to SEES 620 from there. With FPMs, DNCS 507 uses the EA TED 2425(j) for the EA 2409(j) to which the FPM is addressed to do the decryption and authentication and sends decrypted FPM contents 2412 to EA 2409(j). DNCS 507 treats CAA EMMs the same way as EA EMMs, except that the encryption and digest making is done using CAA TED 2427.

DNCS 507 also contains a database of encrypted entity information 2419, which comprises encrypted copies of the private keys and MSKs stored in the TEDs 609 that are connected to DNCS 507. This encrypted entity information is used to restore a TED if a malfunction or the physical destruction of the TED should cause loss of the key information. The encryption is done in the TED using a pass phrase. When the information has been encrypted, it is output to DNCS 507 and stored in database 2419; when the TED is restored, the information is input together with the pass phrase to the TED, which then decrypts the key information.

Detailed Implementation of TED 2425(i): FIG. 25

FIG. 25 is a detailed block diagram of a preferred embodiment of an EA TED 2425(i). In the preferred embodiment, EA TED 2425(i) is implemented using a standard computer motherboard and chassis with a standard Ethernet board and additional means for accelerating RSA encryption and decryption.

As shown in FIG. 25, the main components of TED 2425(i) are CPU 2501, memory 2505, a hardware random number generator 2537, an Ethernet board 254 1, and a number of RSA accelerator boards 2539(0 . . . n), all interconnected by bus 2503. The use of more than one RSA accelerator board 2549 permits RSA encryption and/or decryption in parallel; in consequence, the preferred embodiment of TED 2425(i) is capable of encrypting a plurality of EMMs very rapidly, e.g., within a second, while also performing other operations involving encryption, digest making, or decryption at a similar rate.

Memory 2505 contains EA information 2507, which is the public and private key for the entitlement agent to which TED 2425(i) belongs, the MSKs for the EA, and code 2523, which is the code executed by CPU 2501. The parts of memory 2505 which contain code 2523 and EA information 2507 are non-volatile, with the part containing code 2523 being read-only and the part containing EA information 2507 being both readable and writable. The code which is of interest to the present discussion includes:

- (1) MSK generating code 2525, which generates MSKs and ISKs from random numbers provided by random number generator 2537;
- (2) RSA key generator 2517, which generates public and private RSA keys from random numbers;
- (3) MD5 code 2529, which performs the MD5 one-way hash algorithm;
- (4) 3DES code 2531, which does 3DES encryption and decryption;
- (5) GBAM authorization code 2533, which makes the shared-secret digest used to authenticate global broadcast messages;
- (6) RSA encryption/decryption code 2535, which performs RSA encryption/decryption with the assistance of RSA hardware 2539;
- (7) EA information encryption code 2536, which encrypts EA information 2507 with a pass phrase for storage in DNCS 507;
- (8) EMM code 2538, which produces encrypted and authenticated EMMs; and
- (9) FPM code 2540, which decrypts and checks FPMs.

EA information 2507 contains the information needed to do the encryption and authentication of GBAMs and EMMs sent on behalf of the EA represented by TED 2425(i). EA information 2507 also facilitates and contains information for decryption and authenticity checking on FPMs directed to that EA. In a preferred embodiment, EA information 2507 includes at least: (1) EAID 2509, which is the EAID for EA 2409(i), EA Ku 2511 and EA Kr 2513, which are the public and private keys respectively for EA 2409(i), and (2) a MSK entry (MSKE) 2515 for each MSK being used by EA 2409(i) in conditional access system 601 to which TED 2425(i) belongs. Each MSKE 2515 contains MSK identifier 2517 for the MSK, the expiration time 2519, if any, for the MSK, MSK parity 2520 for the MSK, and MSK 2521 itself. Operations Performed by EA TED 2425(i)

When EA TED 2425(i) is initialized, it is provided with the EAID for the EA to be represented by TED 2425(i). It stores the EAID at 2509 and uses RSA key generation code 2517 and a random number from random number generator 2537 to generate EA public key 2511 and EA private key 2513, which are stored in EA Information 2507. A Remote Procedure Call (RPC) permits DNCS 507 to read EA public key 2511. Other RPCs permit DNCS 507 to read TED 2425(i)'s serial number, to get and set TED 2425(i)'s system time, and to call TED 2425(i) to determine whether it is responding. TED 2425(i) responds to this call with its serial number. EA TED 2425(i) also reports a number of alarm conditions to DNCS 507. These include encryption partial and total failure, random number generation failure, memory failure, and TED and Ethernet overload.

Continuing with the encryption and authentication of EMMs, DNCS 507 has two RPCs, one for EMMs generally and one for MSK EMMs. When DNCS 507 is to make a non-MSK EMM for EA 2409(i), it receives the following from EA 2409(i):

- (1) the serial number of the DHCT 333 which is the destination of the EMM;
- (2) an EAID for EA 2409(i);
- (3) the EMM's type; and
- (4) the information needed for an EMM of that particular type, for example, an entitlement bit map together with the first entitlement ID, the expiration date, and the no-expiration date flag.

DNCS 507 uses the serial number to look up the public key for the DHCT 333 in public key database 2421, uses the

EAID to determine which TED 2425 to use, formats the information as required for an EMM of this type, and provides the formatted information (1123, 1125, and 1127 in FIG. 11) via the RPC to TED 2425(i) together with the DHCT's public key. EMM code 2538 then uses MD5 code 2529 to make a digest of the formatted information and uses RSA E/D code 2535 to encrypt the formatted information with the DHCT's public key and encrypt the digest with private key 2513 for the EA. The encrypted formatted information and the encrypted digest are provided to DNCS 507, which adds whatever else is necessary and places the EMM in EMM database 2420.

For an MSK EMM, DNCS 507 receives the EAID, the DHCT serial number, the EMM type, the MSK parity, the MSKID, and any expiration date from EA 2409(i). DNCS 507 then retrieves the DHCT serial number, formats the information, and makes the RPC call as just described. In this case, EMM code 2538 looks in EA Information 2507 to find the MSK corresponding to the MSK ID and adds the MSK to the formatted information. Then EMM code 2538 uses MD5 code 2529 to make a digest of the formatted information. EMM code 2538 then uses RSA encryption/decryption code to encrypt the formatted information with the DHCT's public key and encrypt the digest with the EA's private key and returns the EMM to DNCS 507, as described above.

The interface for giving a global broadcast message its authentication information requires the MSKID of the MSK that is to be the shared secret and the contents of the global broadcast message. GBAM authorization code 2533 in TED 2425(i) uses the MSKID to locate MSKE 2525 for the MSK, combines MSK 2521 with the contents of the global message (GBAM header 1807 and global broadcast data 1809 in FIG. 18), and uses MD5 code 2529 to produce the digest (GBAM MAC 1805), which it returns to DNCS 507.

With messages sent from the DHCT 333 to the EA, such as the forwarded purchase message, the IP packet in which the message is sent includes the IP address of the DHCT 333 which is the source of the message and that in turn includes the serial number of DHCT 333. DNCS 507 uses the serial number to locate the public key for DHCT 333 in public key database 2421 and provides the public key to TED 2425(i) together with encrypted envelope key 2103, CA FPM message 2105, and FPM signed authentication 2107 from the FPM. FPM code 2540 then:

- (1) uses EA public key 2511 and RSA encryption/decryption code 2535 to decrypt FPM encrypted envelope key 2103;
- (2) uses 3DES code 2531 and the decrypted envelope key to decrypt FPM encrypted events 2113;
- (3) uses RSA encryption/decryption code 2535 and the public key for DHCT 333 to decrypt FPM authentication 2107; and
- (4) uses the decrypted encrypted events with MD5 code 2529 to produce a new hash which it compares with the decrypted value of FPM authentication 2107. If this comparison indicates that the FPM is authentic, TED 2425(i) returns the decrypted events to DNCS 507, which in turn forwards them to EA 2409(i).

The MSKs in MSK 2515 are generated by TED 2425(i). The interface for MSK generation simply requires the MSKID for the new MSK, the parity for the new MSK, and any expiration time. MSK generation code 2525 receives a random number from random number generator 2537 and uses it to generate the new MSK. Then the MSKE 2515 for the new MSK is made and added to EA information 2507. If there is already an MSKE 2525 for the MSKID for the

new MSK, the new MSKE replaces the existing MSKE. TED 2425(i) also generates interactive session keys for the add interactive session EMM. Key generation is as described for the MSK EMM. Once TED 2425(i) has provided the EMM content with the encrypted key to DNCS 507, it overwrites the area in memory 2505 where the interactive session key was stored.

CAA TEDs

CAA TEDs 2427 have the same hardware as EA TEDs, but in the preferred embodiment, they only encrypt the CAA EMMs used to establish an entitlement agent in a DHCT 333. EMM encryption is done exactly as described for EA TEDs. The only keys required for encrypting and authenticating CAA TEDs are the DHCT 333's public key and the CAA's private key. They therefore need only store one of the three public-private key pairs that represent the CAA. The CAA public-private key pair is generated elsewhere. The private key is encrypted using a pass phrase that is provided to CAA TED 2405 along with the key pair. CAA TED then decrypts the private key and stores the decrypted private key, but not the pass phrase, in memory 2505. The encrypted private key, but not the pass phrase, is stored in encrypted entity information 2419 in DNCS 507 as well.

Authenticating Data for Applications Running on DHCT 333: FIG. 23

The foregoing has disclosed how conditional access system 601 uses the conditional access authority, the entitlement agents, DHCTSE 627, and transaction encryption device 603 to provide security for its own operations and for the keys and entitlement information required to decrypt an instance of a service. Another function of conditional access system 601 is that of ensuring secure data downloads for applications executing on DHCT 333. There are two paths by which data may be downloaded: (1) in an MPEG-2 stream via the high bandwidth path running from SEES 619 via transport network 517 to HFC network 521 to DHCT 333, and (2) in IP packets via the lower bandwidth path running from control suite 607 via LAN interconnect device 617 and QPSK modulator 621 to HFC network 521 and DHCT 333.

As with the data used in conditional access system 601, there are two aspects to the problem: security and authentication. Security may be attained by encrypting the data. In the case of data delivered by the high bandwidth path, encryption may be either by DES using an MSK when the data is intended for all DHCTs 333 having a given entitlement agent or by means of the public key for the DHCT when the data is intended for a specific DHCT 333. In the case of data delivered via the lower bandwidth path, the data is addressed to the IP address of a specific DHCT 333 and may be encoded with the public key of the DHCT 333. In the case of encryption with a MSK, the MSK is provided by transaction encryption device 603, and, in the case of encryption with the public key of the DHCT 333, transaction encryption device 603 can provide the key or do the encryption itself. DHCTSE 627 contains the keys needed to do the necessary decryption in DHCT 333.

The authenticating entities in conditional access system 601 comprise the conditional access authority and the entitlement agents. Authentication of downloaded data is done in the same fashion as in EMMs, namely by using a one-way hash function to make a digest of the downloaded data and then encrypting the digest with the private key of the authenticating entity to make a sealed digest. In the preferred embodiment, the sealed digest is made in transaction encryption device 603. When the downloaded data arrives in DHCT 333, DHCTSE 627 uses the public key of

the authenticating entity to decrypt the sealed digest and then uses the one-way hash function to again hash the downloaded data. If the downloaded data is authentic and has not been corrupted in transit, the decrypted sealed digest and the result of hashing the data in the one-way hash function will be equal. It should be noted at this point that the authentication is done not by the originator of the data, but rather by a CAA or EA that is known to the digital broad band delivery system. Moreover, because the CAA or EA is already known to DHCT 333, downloading of authenticated data to DHCT 333 can occur without intervention of the user of DHCT 333.

There are many ways of relating the authentication to the data being authenticated. One way is to use a GBAM as described above with regard to FIG. 20. In such a case, the GBAM payload 2003 would be the digest for the data being downloaded and entitlement agent 2005 would encrypt the digest with its private key as well as making a digest using payload 2003 and a MSK. Another way is to simply send a message via the MPEG-2 transport stream or using an IP packet that contained an authentication portion as well as the data.

One kind of data that can be downloaded using the above techniques is code to be executed by the general purpose processor in DHCT 333. The memory used by the processor includes a portion which is flash memory. That is, the memory cannot be written to like ordinary writable memory, but can be rewritten only as a whole. Such memory is typically used to hold downloadable code. FIG. 23 shows a message containing downloadable code. Code message 2301 has two parts: authentication part 2303 and code part 2305. Code part 2305 contains encrypted or unencrypted code, as the situation requires. Authentication part 2303 contains at least two items of information: authenticator identifier (AID) 2307 and sealed digest 2309. Authenticator identifier 2307 is the CAAID or EAID for the conditional access authority or entitlement agent that is authenticating code 2305; sealed digest 2309 is made by hashing code 2305 in a one-way hash function to make a digest and then encrypting the digest with the private key of the CAA or EA that is authenticating the code. SD 2309 is produced in a preferred environment by a transaction encryption device 605.

Code message 2301 can be sent either in a MPEG-2 transport stream or as an IP packet. Message 2301 may be broadcast to any DHCT 333 that has the authenticating CAA or EA, or it may be sent to a specific DHCT 333. In that case, the packet(s) carrying code message 2301 will include an address for DHCT 333. In the preferred embodiment, the address is DHCT 333's serial number. When code message 2301 arrives in the DHCT 333 for which it is intended, code executing on the processor performs the one-way hash function on code 2305 and provides the result together with AID 2307 and sealed digest 2309 to DHCTSE 627. DHCTSE 627 uses AID 2307 to locate the public key for the CAA or EA and then uses the public key to decrypt sealed digest 2309. Finally, it compares the hash value in decrypted sealed digest 2309 with that provided by the code executing on the processor, and, if they are equal, DHCTSE 627 signals that the code has been authenticated.

Public Key Hierarchy (FIG. 28)

The various elements of the system described herein collectively implement a public key hierarchy 2801 within the network. This is advantageous because such a hierarchy can be used to establish the "trust chains" that support scaleable and spontaneous commercial interaction between DHCTs 333 and other networks that employ public key-

based security, such as the Internet. It can also be used to establish trust in user commercial interactions with the DBDS 501.

FIG. 28 shows the hierarchy of public key certification in the DBDS. There are two independent "trust chains" shown. On the left hand side is the "DHCT chain", which establishes the validity of the public keys associated with DHCTs 333 and enables trusted use of digital signatures made by the DHCT 333. On the right hand side, is the "Operator chain" which establishes the validity of public keys associated with the network operators and the subtending EAs within each system and enables trusted use of signatures of these entities.

The DHCT signature 2806 may be used as described elsewhere herein to authenticate messages sent from the DHCT 333. However, for recipients to be able to trust such DHCT signatures as authentic, they must know with certainty that the public key claimed to be associated with DHCT 333 is in fact the true key which matches with the DHCT's private key. This is accomplished by certifying the DHCT certificate 2806 with the factory programmer certificate authority (FPCA) signature. The FPCA signature can be trusted because reference can be made to FPCA certificate 2805. The DHCT certificates 2806 and the FPCA signature as well as the FPCA certificate 2805 are preferably made at the manufacture time of DHCT 333 in a secure way. Since it may be necessary over time to issue new FPCA certificates and use new FPCA signatures, each FPCA certificate is also certified with a signature of the DHCT Root which may have its own certificate 2804. Said DHCT root certificate 2804 may either be self-signed or may be certified by another authority. DHCT root signature is preferably administered in a highly tamper-resistant device, such as one that meets the requirements of FIPS 140-1 Level 3 certification.

In the operator chain, the various EA certificates 2803 are used to make signatures in the manner described elsewhere herein. Likewise, the Operator CAA signature using the Operator CAA certificate 2802 is used to certify each EA signature as described previously herein. Above the operator CAA signature, two Root CAA signatures may be used to introduce an operator CAA 2802 to a DHCT 333 in a secure way. In fact, preferably at manufacture time, there are three Root CAA public keys placed into the secure NVM of the DHCT 333. Then, authentic messages from any two of the Root CAAs may be used to replace the third Root CAA public key with that of the Operator CAA whose key is certified in Operator CAA certificates 2802. The Root CAA is preferably administered by the manufacturer in a tamper-resistant device that meets or exceeds the requirements of FIPS 140-1 Level 3 certification. It is possible, however, through an appropriate sequence of messages, to change all of the Root CAA public keys to be those of other CAAs that the manufacturer has no control over. It is thus possible to remove the manufacturer from the signature chain. In this case, the Root CAA can be some other organization approved by one or more operators or it may be administered by an operator.

As shown in FIG. 28 and described elsewhere herein, each operator may have a plurality of EAs. In a preferred embodiment, there is a different EA and an associated EA certificate 2803 for every operating site of any given operator. This ensures that DHCTs can not be migrated between operational sites without the knowledge and participation of the operator CAA signature 2802.

The geo-political CA certificate 2807 shown in FIG. 28, is not required to operate the normal conditional access and electronic activities of the operator. However, the operator may desire to link its signature chain into a larger chain to

be able to participate or have DHCTs 333 participate in transactions involving entities outside of the operator's DBDS. In this case, the signature chains may be readily linked to those of geo-political CA and its signature 2807 by having the public keys of one or all of the DHCT root signature 2804, the Root CAA signature 2808 or operator CAA signatures 2802 certified by the geo-political CA signature. This is accomplished by having a certificate placed in a database for each of the public keys associated with signatures 2804, 2808 and 2802. Said certificate is signed with the private key of the geopolitical CA 2807.

FIG. 29 shows an EMM generator 2901. As described elsewhere herein, it is preferred that DHCTs 333 that are operated by different operators in different DBDS instances are controlled by an operator CAA that is specific to that operator and system. Since DHCTs 333 at manufacture time are not configured to be controlled by any operator CAA, but instead are controlled by three Root CAAs the public keys of which are placed in the memory of the secure processor during manufacture, they must be reconfigured for control by different operators. This must be done securely. As described elsewhere herein, messages bearing the digital signatures of two of the Root CAAs can be used to reconfigure the terminal with respect to the third CAA. The EMM generator 2901 is used to produce one of the two messages needed to introduce a new Operator CAA public key in a certified way to the DHCT 333. DHCT public key certificates 2902 are input to the EMM generator so that it may know for which DHCTs messages are to be made. The DHCTs that will be controlled by a specific operator may be placed in a separate file of the input device or may be associated with an operator in other ways clear to those skilled in the art.

Prior to generating introductory EMMs 2903, certified public keys of the various operators served by the EMM Generator 2901 are loaded into the public key memory 2904 of the EMM Generator 2901. Thus, when EMM generator 2901 reads input of DHCTs needed to be introduced to Operator A, the EMM generator uses the public key of Operator A read from memory 2904 to produce EMMs containing the public key of Operator A. Likewise, prior to generating introductory EMMs 2903, the private keys of the Root CAAs must be loaded into the private key memory 2905 of the EMM generator 2901. Said EMMs are digitally signed by the EMM Generator 2901 using the private keys of the Root CAAs contained in memory 2905. Since private signing keys are contained in memory 2905 of EMM Generator 2901, the EMM Generator 2901 must be implemented in a secure fashion that prevents discovery of the values of the Root CAA private keys stored in memory 2905. EMM Generator 2901 should thus be implemented in a tamper-resistant device which meets the requirements of FIPS 140-1 Level 3 or higher.

Since two Root CAA private keys must be used to sign separate CAA Introductory EMMs 2903, there are preferably two EMM Generators 2901 implemented, one each for each of the two Root CAA private keys. It is also preferred that EMM generators 2901 are operated in separate physical facilities.

The Detailed Description of a Preferred Embodiment set forth above is to be regarded as exemplary and not restrictive, and the breadth of the invention disclosed herein is to be determined from the claims as interpreted with the full breadth permitted by the patent laws.

What is claimed is:

1. A method of decrypting an instance of a service that has been encrypted with a short-term key, the method being

49

carried out in a receiver that has a public key-private key pair and the method comprising the steps of:

- receiving a first message in the receiver whose contents include a long-term key, the contents having been encrypted using the public key for the receiver; 5
 - using the private key to decrypt the contents;
 - storing the long-term key;
 - receiving a second message in the receiver together with the instance of the service, the second message including a key derivation value; 10
 - using the key derivation value and the long-term key to obtain the short-term key; and
 - using the short-term key to decrypt the instance of the service. 15
2. The method set forth in claim 1 wherein:
- the receiver includes a secure element in which the private key is stored;
 - the steps of decrypting the contents, storing the long-term key, and using the long-term key and the key derivation value to obtain the short-term key are carried out in the secure element. 20
3. The method set forth in claim 1 wherein the first message further includes first authentication information; and the method further comprises the steps of: 25
- using the first authentication information to determine whether the first message is authentic; and
 - disregarding the first message if the first message is not authentic. 30
4. The method set forth in claim 3 wherein:
- the receiver has a public key for an entitlement agent;
 - the first authentication information is a digest of information in the first message, the digest being encrypted with a private key corresponding to the public key for the entitlement agent; and 35
- the step of using the first authentication information includes the steps of:
- making a new digest of the information in the first message; 40
 - decrypting the first authentication information; and
 - comparing the new digest with the decrypted first authentication information, the first message being authentic when the two are the same.
5. The method set forth in claim 4 wherein: 45
- the receiver includes a secure element in which the public key for the entitlement agent and the private key for the receiver are stored; and
 - the steps of decrypting the contents, storing the long-term key, using the first authentication information, and using the long-term key and the key derivation value to obtain the short-term key are carried out in the secure element. 50
6. The method set forth in claim 1, wherein: 55
- the first message and the second message each includes an indication of an entitlement agent;
 - the step of storing the long-term key includes the step of associating the long-term key with the entitlement agent identified by the indication in the first message; 60
 - and
 - the method further comprises the step of using the indication of the entitlement agent in the second message to locate the stored long-term key.
7. The method set forth in claim 6, wherein: 65
- the first message and the second message each further includes a key identifier for the long-term key;

50

the step of storing the long-term key further includes the step of associating the long-term key with the key identifier from the first message; and

the method further comprises the step of using the key identifier from the second message to locate the long-term key.

8. The method set forth in claim 7 wherein:

the second message further includes an entitlement specifier specifying an entitlement; and

the method further comprises the steps of:

- receiving a third message in the receiver, the contents of the third message including an entitlement agent specifier and an entitlement specifier and the contents of the third message having been encrypted using the public key for the receiver;

- using the private key to decrypt the contents of the third message;

- storing the entitlement specifier in association with the entitlement agent specified by the entitlement agent specifier; and

- determining whether the entitlement specifier in the second message matches a stored entitlement specifier associated with the entitlement agent specified in the second message, and performing the step of using the key derivation value and the long-term key to obtain the short-term key only if a match is found.

9. The method set forth in claim 8 wherein:

- there is a plurality of entitlement agents;

- a plurality of long-term keys are associated with a given entitlement agent; and

- a plurality of entitlements are associated with a given entitlement agent.

10. The method set forth in claim 8 wherein:

- the receiver includes a secure element in which the private key for the receiver is stored; and

- the secure element performs the steps of decrypting the contents of the first message; decrypting the contents of the third message; storing the long-term key; storing the entitlement specifier in association with the entitlement agent; using the indication of the entitlement agent; determining whether the entitlement specifier in the second message matches a stored entitlement specifier; using the key identifier from the second message to locate the long-term key; and using the key derivation value and the long-term key to obtain the short-term key.

11. The method set forth in claim 6 wherein:

- the second message further includes an entitlement specifier; and

the method further comprises the steps of:

- receiving a third message in the receiver, the contents of the third message including an entitlement agent specifier and an entitlement specifier and the third message having been encrypted using the public key for the receiver;

- using the private key to decrypt the contents of the third message;

- storing the entitlement specifier in association with the entitlement agent specified by the entitlement agent specifier; and

- determining whether the entitlement specifier in the second message matches a stored entitlement specifier associated with the entitlement agent specified in the second message, and performing the step of using the key derivation value and the long-term key to obtain the short-term key only if a match is found.

51

12. The method set forth in claim 11 wherein:
there is a plurality of entitlement agents; and
a plurality of entitlements are associated with a given
entitlement agent.

13. The method set forth in claim 11 wherein:
the receiver includes a secure element in which the private
key for the receiver is stored; and
the secure element performs the steps of
decrypting the contents of the first message,
decrypting the contents of the second message,
storing the long-term key,
storing the entitlement specifier in association with the
entitlement agent,
using the indication of the entitlement agent,
determining whether the entitlement specifier in the
second message matches a stored entitlement speci-
fier; and
using the key derivation value and the long-term key to
obtain the short term key.

14. The method set forth in claim 9 wherein:
the third message further includes authentication infor-
mation; and
the method further comprises the steps of:
using the authentication information to determine
whether the third message is authentic; and
disregarding the third message if it is determined that
the third message is not authentic.

15. The method set forth in claim 14 wherein:
the receiver has a public key for an entitlement agent;
the authentication information is a digest of information
in the third message which has been encrypted with a
private key corresponding to the public key for the
entitlement agent; and
the step of using the first authentication information
includes the steps of:
making a new digest of the information in the third
message;
decrypting the authentication information; and
comparing the new digest with the decrypted authen-
tication information, the third message being authen-
tic if the two are the same.

16. A method of enabling a receiver that has a public key
to decrypt an instance of a service that has been encrypted
with a short-term key, the method comprising the steps of:
using the public key to encrypt contents of a first message,
the contents including a long-term key;
sending the first message to the receiver;
sending a second message to the receiver together with
the encrypted instance of the service, the second mes-
sage including a key derivation value; and
the receiver responding to the first message by decrypting
the contents and storing the long-term key and respond-
ing to the second message by using the key derivation
value and the long-term key to obtain the short-term
key and using the short-term key to decrypt the instance
of the service.

17. The method set forth in claim 16 wherein the public
key for the receiver is stored in a certified form.

18. The method set forth in claim 16 further comprising
the steps of:
obtaining the long-term key from a secure element in
which it is stored; and
using the long-term key to produce the short-term key.

19. The method set forth in claim 16 further comprising
the step of:

52

adding first authentication information to the first
message, wherein the receiver uses the first authenti-
cation information to check the authenticity of the first
message and stores the long-term key in response to the
first message only if the authenticity of the first mes-
sage is confirmed.

20. The method set forth in claim 19 wherein:
the receiver has a public key for an entitlement agent;
the step of adding first authentication information
includes the step of making an encrypted digest of
information in the first message, the digest being
encrypted with a private key corresponding to the
public key for the entitlement agent, and
the receiver checks the authenticity of the first message by
making a new digest of the information in the first
message, using the public key for the entitlement agent
to decrypt the first authentication information, and
comparing the new digest with the decrypted first
authentication information, the first message being
authentic if the two are the same.

21. The method set forth in claim 20, further comprising
the step of:
adding second authentication information to the second
message, the receiver using the second authentication
information to determine whether the second message
is authentic and disregarding the second message if the
second message is not authentic.

22. The method set forth in claim 21 wherein:
the second message is associated with an entitlement
agent;
the step of adding second authentication information
includes the step of making a digest of information in
the second message and a secret shared by the entitle-
ment agent and the receiver; and
the receiver checks the authenticity of the second message
by making a new digest of the information in the
second message and the shared secret and comparing
the new digest with the digest of the second message,
the second message being authentic if the two are the
same.

23. The method set forth in claim 22 wherein:
the shared secret includes at least a portion of the long-
term key.

24. The method set forth in claim 23 wherein:
the long-term key is stored in a secure element; and
the step of making the digest is carried out in the secure
element.

25. The method set forth in claim 20 wherein:
the private key for the entitlement agent and the long-term
key are stored in a secure element;
the public key is stored in a certified form; and
the steps of using the public key for the receiver to encrypt
the first message and making the encrypted digest are
carried out in the secure element.

26. The method set forth in claim 25 further comprising
the steps of:
obtaining the long-term key from the secure element; and
using the long-term key to produce the short-term key.

27. The method set forth in claim 16 wherein:
the first message and the second message each includes an
indication of an entitlement agent; and
the receiver further responds to the first message by
associating the long-term key with the entitlement
agent identified by the indication in the first message

53

and responds to the second message by using the indication of the entitlement agent in the second message to locate the stored long-term key.

28. The method set forth in claim 27 wherein:

the first message and the second message each further includes a key identifier for the long-term key, the receiver further responding to the first message by associating the long-term key with the key identifier from the first message and responding to the second message by using the key identifier from the second message to locate the long-term key.

29. The method set forth in claim 28 wherein:

the second message further includes an entitlement specifier specifying an entitlement; and

the method further comprises the step of sending a third message to the receiver, the contents of the third message including an entitlement agent specifier and an entitlement specifier and the contents of the third message having been encrypted using the public key for the receiver; and

the receiver responds to the third message by using the private key to decrypt the contents of the third message, storing the entitlement specifier in association with the entitlement agent specified by the entitlement agent specifier, determining whether the entitlement specifier in the second message matches a stored entitlement specifier associated with the entitlement agent specified in the second message, and performing the step of using the key derivation value and the long-term key to obtain the short-term key only if a match is found.

30. The method set forth in claim 29 wherein:

there is plurality of entitlement agents;

a plurality of long-term keys are associated with a given entitlement agent; and

a plurality of entitlements for at least one receiver are associated with a given entitlement agent.

31. The method set forth in claim 27 wherein:

the second message further includes an entitlement specifier specifying an entitlement; and

the method further comprises the step of sending a third message to the receiver, the contents of the third message including an entitlement agent specifier and an entitlement specifier and the contents of the third message having been encrypted using the public key for the receiver, the receiver responding to the third message by using the private key to decrypt the contents of the third message, storing the entitlement specifier in association with the entitlement specifier in the second message matches a stored entitlement specifier associated with the entitlement agent specified in the second message, and performing the step of using the key derivation value and the long-term key to obtain the short-term key only if a match is found.

32. The method set forth in claim 31 wherein:

there is a plurality of entitlement agents; and

a plurality of entitlements are associated with a given entitlement agent.

33. The method set forth in claim 31, further comprising the step of adding authentication information to the third message, the receiver using the authentication information to check the authenticity of the third message and storing the long-term key in response to the third message only if the authenticity of the third message is confirmed.

34. The method set forth in claim 33 wherein:

the receiver has a public key for an entitlement agent;

54

the step of adding authentication information includes the step of making an encrypted digest of information in the third message, the digest being encrypted with a private key corresponding to the public key for the entitlement agent; and

the receiver checks the authenticity of the third message by making a new digest of the information in the third message, using the public key for the entitlement agent to decrypt the authentication information, and comparing the new digest with the decrypted authentication information, the third message being authentic if the two are the same.

35. The method set forth in claim 34 wherein:

the private key for the entitlement agent and the long-term key are stored in a secured element;

the public key is stored in a certified form; and

the steps of using the public key for the receiver to encrypt the third message and making the encrypted digest using the private key are carried out in the secure element.

36. A receiver for receiving and decrypting an instance of a service that has been encrypted with a short-term key, the receiver having a public key, and the receiver comprising:

a memory that contains the private key corresponding to the receiver's public key;

a service decryptor that uses the short-term key to decrypt the instance of the service;

a first message interpreter that responds to a first message received in the receiver, the first message's contents, including a long-term key, having been encrypted using the receiver's public key and the first message interpreter responding to the first message by decrypting the contents and storing the long-term key in the memory; and

a second message interpreter that responds to a second message received in the receiver together with the instance of the service, the second message's contents including a key derivation value and the second message interpreter responding to the second message by using the key derivation value and the long-term key to obtain the short-term key and providing the short-term key to the service decryptor.

37. The receiver set forth in claim 36 further comprising:

a secure element for implementing at least in part, the memory, the first message interpreter, and the second message interpreter and for storing, within the memory, the private key and the long-term key.

38. The receiver set forth in claim 36 wherein:

the first message further includes first authentication information; and

the first message interpreter further responds to the first message by using the first authentication information to determine whether the first message is authentic and disregarding the first message if the first message is not authentic.

39. The method set forth in claim 38 wherein:

a public key for an entitlement agent is stored in the memory;

the first authentication information is a digest of information in the first message, the digest being encrypted with a private key corresponding to the public key for the entitlement agent; and

the first message interpreter determines whether the first message is authentic by making a new digest of the information in the first message, decrypting the authen-

55

tication information, and comparing the new digest with the decrypted first authentication information, the first message being authentic if the two are the same.

40. The receiver set forth in claim 36, wherein:

the second message further includes second authentication information; and

the second message interpreter further responds to the second message by using the second authentication information to determine whether the second message is authentic and disregarding the second message if the second message is not authentic.

41. The receiver of claim 40, wherein:

the second message is associated with an entitlement agent; and

the second message interpreter makes a digest of information in the second message and a secret shared by the entitlement agent and the receiver, wherein the receiver checks the authenticity of the second message by making a new digest of the information in the second message and the shared secret and comparing the new digest with the digest of the second message, the second message being authentic when the two are the same.

42. The method of claim 1, wherein said receiver is included in a set top terminal of a cable television system.

43. The method of claim 42, wherein said instance of service is transmitted in a downstream direction from head end equipment of the cable television system to said set top terminal.

56

44. The method of claim 1, wherein:

said receiver is included in head end equipment of a cable television system;

said first and second messages original in a set top terminal of the cable television system;

said instance of service comprises data generated by said set top terminal; and

said long term key comprises a session key.

45. The method of claim 44, wherein said data is transmitted upstream, through the cable television system, from said set top terminal to said head end equipment.

46. The method of claim 1, wherein:

said first message comprises an entitlement management message including authorization information;

said second message comprises an entitlement control message including service identification information that identifies the instance of service; and

said instance of service is decrypted only when said service identification information is equivalent to said authorization information, thereby preventing replay attacks on said instance of service.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,157,719
DATED : December 5, 2000
INVENTOR(S) : Wasilewski et al.

Page 1 of 3

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 1,

Line 8, delete "08/6,005,938" and insert therefor -- 6,005,938 --
Line 25, delete "abnd" and insert therefore -- and --

Column 3,

Line 30, delete "DHSTSE" and insert therefore -- DHCTSE --

Column 8,

Line 31, delete both occurrences of DHICT" and insert therefore -- DHCT --

Column 9,

Line 9, delete "counterbased" and insert therefore -- counter-based --

Column 16,

Line 62, delete "FMMs" and insert therefore -- EMMs --

Column 17,

Line 55, delete "FCM" and insert therefore -- ECM --
Line 62, delete "scaled" and insert therefore -- sealed --

Column 19,

Line 58, delete "705(c)" and insert therefore -- 705(e) --

Column 20,

Line 54, delete "DHCTSF" and insert therefore -- DHCTSE --

Column 21,

Line 10, delete "DHCTSF" and insert therefore -- DHCTSE --

Column 22,

Line 6, delete "dccryption" and insert therefore -- decryption --

Column 24,

Line 25, delete "scaled" and insert therefore -- sealed --

Column 27,

Line, 1 delete "space." and insert therefore -- space, --

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,157,719
DATED : December 5, 2000
INVENTOR(S) : Wasilewski et al.

Page 2 of 3

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 31,

Line 38, delete "NVSC." and insert therefore --NVSC, --

Line 58, delete "FMM" and insert therefore "EMM"

Column 32,

Line 31, delete "discussion" and insert therefore -- discussion,"

Column 36,

Line 43, delete "comer" and insert therefore -- corner --

Column 37,

Line 63, delete "DHCTSF" and insert therefore --DHCTSE --

Column 38,

Line 8, delete "description when" and insert therefore -- description, when --

Column 40,

Line 20, delete "MPFG-2" and insert therefore --MPEG-2 --

Column 42,

Line 50 delete "254 1" and insert therefore --2541 --

Column 43,

Line 18, delete "507," and insert therefore --507; --

Column 46,

Line 29, delete "downloadabl" and insert therefore -- downloadable --

Lines 54-55, delete DfICTSE" and insert therefore -- DHCTSE --

Column 48,

Line 11, delete "geopolitical" and insert therefore -- geo-political --

Column 49,

Line 21, delete "longterm" and insert therefore -- long-term --

Line 53, delete "arc" and insert therefore -- are --

Column 50,

Line 7, delete "wherein:" and insert therefore -- wherein; --

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,157,719
DATED : December 5, 2000
INVENTOR(S) : Wasilewski et al.

Page 3 of 3

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 54,

Line 58, delete "method" and insert therefore -- receiver --

Signed and Sealed this

Second Day of October, 2001

Attest:

Nicholas P. Godici

Attesting Officer

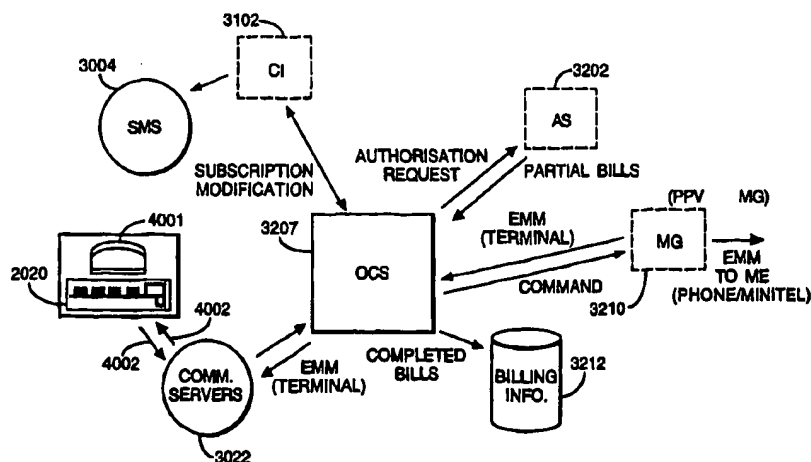
NICHOLAS P. GODICI
Acting Director of the United States Patent and Trademark Office



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04N 7/16, 7/167	A1	(11) International Publication Number: WO 98/43426
		(43) International Publication Date: 1 October 1998 (01.10.98)
<p>(21) International Application Number: PCT/EP97/02108</p> <p>(22) International Filing Date: 25 April 1997 (25.04.97)</p> <p>(30) Priority Data: 97400650.4 21 March 1997 (21.03.97) EP</p> <p>(34) Countries for which the regional or international application was filed: FR et al.</p> <p>(71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André Citroën, F-75711 Paris Cedex 15 (FR).</p> <p>(72) Inventors; and</p> <p>(75) Inventors/Applicants (for US only): BAYASSI, Mulham [FR/FR]; 30, rue de Chambéry, F-75015 Paris (FR). DE LA TULLAYE, Pierre [FR/FR]; 7, allée Marcel Jouhandeau, F-92500 Rueil Malmaison (FR). JEZEQUEL, Jean-François [FR/FR]; 35, rue du Commandant Kieffer, F-95240 Comaille en Paris (FR).</p> <p>(74) Agent: COZENS, Paul, Dennis; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).</p>		<p>(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Published With international search report.</p>

(54) Title: BROADCAST AND RECEPTION SYSTEM, AND CONDITIONAL ACCESS SYSTEM THEREFOR



(57) Abstract

A digital satellite television system has a plurality of set-top-boxes associated with a plurality of end users' television receivers, a modem and a decoder housed in each STB, a Subscriber Authorization System (SAS) incorporating or having associated therewith a plurality of communication servers, means included in the SAS for generating Electronic Managements Messages (EMM), a back channel interconnecting each of the STBs individually with the SAS, means included in the SAS and each STB so that the necessary information required to inject a relevant EMM into the system is supplied directly to the relevant communication server included in or associated with the SAS to authorise the release of the said EMM and/or means to connect the modem to the back channel and means whereby an EMM is transmissible to the decoder directly from a relevant communication server included in or associated with the SAS. Further important features are also disclosed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

- 1 -

**BROADCAST AND RECEPTION SYSTEM, AND CONDITIONAL ACCESS
SYSTEM THEREFOR**

5 The present invention relates to a broadcast and reception system, in particular to a mass-market digital interactive satellite television system, and to a conditional access system therefor.

In particular, but not exclusively, the invention relates to a mass-market broadcast system having some or all of the following preferred features:-

- It is an information broadcast system, preferably a radio and/or television broadcast system
- 10 ● It is a satellite system (although it could be applicable to cable or terrestrial transmission)
- It is a digital system, preferably using the MPEG, more preferably the MPEG-2, compression system for data/signal transmission
- It affords the possibility of interactivity.

15 More particularly the present invention relates to so-called pay television (or radio) where a user/viewer selects a programme/film/game to be viewed for which payment is to be made, this being referred to as a pay-per-view (PPV) or in the case of data to be downloaded a so-called pay-per-file (PPF).

20 With such known PPV or PPF systems a significant amount of time is required to be spent by the user/viewer in order to carry out the actions necessary to actually access the product being selected.

For example, in one known system the sequence of steps which have to be carried out are as follows:-

- I) The user telephones a so-called Subscriber Management System (SMS)
- 25 which in this known system includes a number of human operators which answer the subscriber's call and to whom the subscriber communicates the necessary information concerning the selected product and concerning the financial status of the subscriber

- 2 -

to a so-called Subscriber Authorization System (SAS) which has included in it or associated with it a plurality of communications servers.

- ii) The operator at the SMS then has to check the financial status of the user before authorising the connection from the communications servers to the user's television set so that the product can be delivered and viewed by the user.

In another known system the human operator is replaced by an automatic voice server so that when the user telephones the SMS he/she hears a voice activated recording to which the user conveys the same information as in above.

- This second arrangement reduces the delay inherent in the first described arrangement which can be more easily overloaded when large numbers of users are wishing to order a product at the same time.

However, even with this second arrangement the user is involved in inputting significant information in the form of lengthy serial numbers which operation provides plenty of scope for error as well as being time consuming.

- The third known arrangement involves the user making use of existing screen based systems such as MINITEL in France and PRESTEL in the United Kingdom, which systems replace the voice activated server referred to above in connection with the second arrangement. The MINITEL and PRESTEL systems themselves incorporate a modem at the consumer end.

- In all these known arrangements the user is involved in the expenditure of significant time and effort in inputting all the information necessary to enable the system to in effect authorize the transmission of the chosen product to the user's television set.

In the case of a satellite television system there is a further delay involved in the user actually receiving the product selected.

- 3 -

In PPV and PPF systems the key element in controlling the user's access to products are so-called Entitlement Management Messages (EMM) which have to be injected into the system in order to give the user product access. More particularly the EMMs are the mechanism by which the encrypted data representative of a product is
5 decrypted for a particular individual user.

In known satellite television systems the EMMs are transmitted to the user's televisions via the satellite link at regular intervals in the MPEG-2 data stream. Thus in the case of a particular user's EMM there can be a significant delay of perhaps several minutes before the user's next EMM transmission arrives at that user's
10 television set.

This transmission delay is in addition to the delay referred to earlier which is inherent in the user having to manually input certain data into the system. The cumulative effect of these two delays is that it may take perhaps typically five minutes for a user to be able to gain access to the selected product.

15 The present invention is concerned with overcoming this problem.

In a first aspect, the present invention provides a conditional access system comprising:

means for generating a plurality of (preferably conditional access) messages;
and

20 means for receiving the messages, said receiving means being adapted to communicate with said generating means via a communications server connected directly to said generating means.

Preferably, the message is an entitlement message for transmission (for example by broadcast) to the receiving means, said generating means being adapted to generate
25 entitlement messages in response to data received from said receiving means.

The generating means may be arranged to transmit a message as a packet of digital

- 4 -

data to said receiving means either via said communications server or via a satellite transponder.

The receiving means may be connectable to said communications server via a modem and telephone link.

- 5 In a related aspect, the present invention provides a conditional access system for affording conditional access to subscribers, comprising:
- a subscriber management system;
 - a subscriber authorization system coupled to the subscriber management system; and
 - 10 a communications server; said server being connected directly to the subscriber authorization system.

The system may further comprise a receiver/decoder for the subscriber, the receiver/decoder being connectable to said communications server, and hence to said subscriber authorization system, via a modem and telephone link.

- 15 In a second aspect, the present invention provides a broadcast and reception system including a conditional access system as described above.

In a third aspect, the present invention provides a broadcast and reception system comprising:

- 20 means for generating a plurality of entitlement messages relating to broadcast programs;
 - means for receiving said messages from said generating means; and
 - means for connecting the receiving means to the generating means to receive said messages, said connecting means being capable of effecting a dedicated connection between the receiving means and the generating means.
- 25 The dedicated connection would typically be a hard-wired connection and/or a modemmed connection, with the possibility of the connection been made via a cellular

- 5 -

telephone system. In other words, the dedicated connection is capable of forming a channel of communication (from point to point). This is in contrast to broadcasting of information through the air or ambient medium. The connecting means would typically be a modem at the receiving means.

- 5 Hence, in a closely related aspect, the present invention provides a broadcast and reception system comprising:

means for generating a plurality of entitlement messages relating to broadcast programs;

means for receiving said messages from said generating means via a modem;

10 and

means for connecting said modem to said generating means and said receiving means.

The above features can afford the advantage of providing the user the necessary viewing authorization (via the EMM) more quickly than has hitherto been possible, partly because, since the SAS typically uses a smaller amount of computer code than the SMS, the SAS can operate more efficiently (and in real time), partly because the SAS can itself, directly, generate the requisite EMM, and partly because the EMM can be passed to the user or subscriber via a dedicated (typically modemmed) link.

20 Preferably, the generating means is connected to said modem via a communications server which is preferably included in or associated with said generating means.

The receiving means may be further adapted to receive said entitlement messages via a satellite transponder.

25 The receiving means may be a receiver/decoder comprising means for receiving a compressed MPEG-type signal, means for decoding the received signal to provide a television signal and means for supplying the television signal to a television.

Preferably, the receiving means is adapted to communicate with said generating means

- 6 -

via said modem and connecting means. The receiving means may comprise means for reading a smartcard insertable therein by an end user, the smartcard having stored therein data to initiate automatically the transmission of a message from said receiving means to said generating means upon insertion of the smartcard by the end user.

In addition, the system may further comprise a voice link to enable the end user of the broadcast and reception system to communicate with the generating means.

It will be understood from the above that the present invention provides two arrangements by which the time it takes for an end user to access a desired product is reduced. Preferably both arrangements are employed to achieve the maximum time saving but either arrangement can be used individually.

According to a further aspect of the present invention, there is provided a broadcast and reception system, comprising, at the broadcast end:

a broadcast system including means for broadcasting a callback request;
and at the reception end:
a receiver including means for calling back the broadcast system in response to the callback request.

By providing that the broadcast system can request the receiver to call it back, the possibility is afforded of the broadcast system obtaining information from the receiver about the state of the receiver.

Preferably, the means for calling back the broadcast system includes a modem connectable to a telephone system. By using a modemmed back channel, a simple way of putting the invention into effect can be provided.

Preferably also, the means for calling back the broadcast system is arranged to transfer to the broadcast system information concerning the receiver. This information might include the number of remaining tokens, the number of pre-booked sessions, and so

- 7 -

on.

Preferably, the broadcast system includes means for storing the information, so that it can be processed at a later time, as desired.

5 Preferably, the broadcast means is arranged to broadcast a callback request which includes a command that the callback be made at a given time, and the means for calling back the broadcast system is arranged to respond to said command. By arranging for the callback to be later than the actual request, greater flexibility can be imparted to the system.

10 The broadcasting means may be arranged to broadcast as the callback request one or more Entitlement Messages for broadcast.

15 Preferably, the broadcast system includes means for generating a check message (such as a random number) and passing this to the receiver, the receiver includes means for encrypting the check message and passing this to the broadcast system, and the broadcast system further includes means for decrypting the check message received from the receiver and comparing this with the original check message. In this way it can be checked whether the receiver is genuine.

Any of the above features may be combined together in any appropriate combination. They may also be provided, as appropriate, in method aspects.

20 Preferred features of the present invention will now be described, purely by way of example, with reference to the accompanying drawings, in which:-

Figure 1 shows the overall architecture of a digital television system according to the preferred embodiment of the present invention;

Figure 2 shows the architecture of a conditional access system of the digital television system;

- 8 -

Figure 3 shows the structure of an Entitlement Management Message used in the conditional access system;

Figure 4 is a schematic diagram of the hardware of a Subscriber Authorisation System (SAS) according to a preferred embodiment of the present invention;

5 Figure 5 is a schematic diagram of the architecture of the SAS;

Figure 6 is a schematic diagram of a Subscriber Technical Management server forming part of the SAS;

Figure 7 is a flow diagram of the procedure for automatic renewal of subscriptions as implemented by the SAS;

10 Figure 8 is a schematic diagram of a group subscription bitmap used in the automatic renewal procedure;

Figure 9 shows the structure of an EMM used in the automatic renewal procedure;

Figure 10 shows in detail the structure of the EMM;

15 Figure 11 is a schematic diagram of an order centralized server when used to receive commands directly through communications servers;

Figure 12 illustrates diagrammatically a part of Figure 2 showing one embodiment of the present invention;

Figure 13 is a schematic diagram of the order centralized server when used to receive commands from the subscriber authorization system to request a callback;

20 Figure 14 is a schematic diagram of the communications servers;

- 9 -

Figure 15 shows the manner in which EMM emission cycle rate is varied according to the timing of a PPV event;

Figure 16 is a schematic diagram of a Message Emitter used to emit EMMs;

Figure 17 is a schematic diagram showing the manner of storage of EMMs within the
5 Message Emitter;

Figure 18 is a schematic diagram of a smartcard;

Figure 19 is a schematic diagram of an arrangement of zones in the memory of the smartcard; and

Figure 20 is a schematic diagram of a PPV event description.

10 An overview of a digital television broadcast and reception system 1000 according to the present invention is shown in Figure 1. The invention includes a mostly conventional digital television system 2000 which uses the known MPEG-2 compression system to transmit compressed digital signals. In more detail, MPEG-2 compressor 2002 in a broadcast centre receives a digital signal stream (typically a
15 stream of video signals). The compressor 2002 is connected to a multiplexer and scrambler 2004 by linkage 2006. The multiplexer 2004 receives a plurality of further input signals, assembles one or more transport streams and transmits compressed digital signals to a transmitter 2008 of the broadcast centre via linkage 2010, which can of course take a wide variety of forms including telecom links. The transmitter
20 2008 transmits electromagnetic signals via uplink 2012 towards a satellite transponder 2014, where they are electronically processed and broadcast via notional downlink 2016 to earth receiver 2018, conventionally in the form of a dish owned or rented by the end user. The signals received by receiver 2018 are transmitted to an integrated receiver/decoder 2020 owned or rented by the end user and connected to the end user's
25 television set 2022. The receiver/decoder 2020 decodes the compressed MPEG-2 signal into a television signal for the television set 2022.

- 10 -

A conditional access system 3000 is connected to the multiplexer 2004 and the receiver/decoder 2020, and is located partly in the broadcast centre and partly in the decoder. It enables the end user to access digital television broadcasts from one or more broadcast suppliers. A smartcard, capable of decrypting messages relating to commercial offers (that is, one or several television programmes sold by the broadcast supplier), can be inserted into the receiver/decoder 2020. Using the decoder 2020 and smartcard, the end user may purchase events in either a subscription mode or a pay-per-view mode.

An interactive system 4000, also connected to the multiplexer 2004 and the receiver/decoder 2020 and again located partly in the broadcast centre and partly in the decoder, enables the end user to interact with various applications via a modemmed back channel 4002.

The conditional access system 3000 is now described in more detail.

With reference to Figure 2, in overview the conditional access system 3000 includes a Subscriber Authorization System (SAS) 3002. The SAS 3002 is connected to one or more Subscriber Management Systems (SMS) 3004, one SMS for each broadcast supplier, by a respective TCP-IP linkage 3006 (although other types of linkage could alternatively be used). Alternatively, one SMS could be shared between two broadcast suppliers, or one supplier could use two SMSs, and so on.

First encrypting units in the form of ciphering units 3008 utilising "mother" smartcards 3010 are connected to the SAS by linkage 3012. Second encrypting units again in the form of ciphering units 3014 utilising mother smartcards 3016 are connected to the multiplexer 2004 by linkage 3018. The receiver/decoder 2020 receives a "daughter" smartcard 3020. It is connected directly to the SAS 3002 by Communications Servers 3022 via the modemmed back channel 4002. The SAS sends amongst other things subscription rights to the daughter smartcard on request.

The smartcards contain the secrets of one or more commercial operators. The

- 11 -

"mother" smartcard encrypts different kinds of messages and the "daughter" smartcards decrypt the messages, if they have the rights to do so.

The first and second ciphering units 3008 and 3014 comprise a rack, an electronic VME card with software stored on an EEPROM, up to 20 electronic cards and one
5 smartcard 3010 and 3016 respectively, for each electronic card, one (card 3016) for encrypting the ECMs and one (card 3010) for encrypting the EMMs.

The operation of the conditional access system 3000 of the digital television system will now be described in more detail with reference to the various components of the television system 2000 and the conditional access system 3000.

10 Multiplexer and Scrambler

With reference to Figures 1 and 2, in the broadcast centre, the digital video signal is first compressed (or bit rate reduced), using the MPEG-2 compressor 2002. This compressed signal is then transmitted to the multiplexer and scrambler 2004 via the linkage 2006 in order to be multiplexed with other data, such as other compressed
15 data.

The scrambler generates a control word used in the scrambling process and included in the MPEG-2 stream in the multiplexer 2004. The control word is generated internally and enables the end user's integrated receiver/decoder 2020 to descramble the programme.

20 Access criteria, indicating how the programme is commercialised, are also added to the MPEG-2 stream. The programme may be commercialised in either one of a number of "subscription" modes and/or one of a number of "Pay Per View" (PPV) modes or events. In the subscription mode, the end user subscribes to one or more commercial offers, or "bouquets", thus getting the rights to watch every channel inside
25 those bouquets. In the preferred embodiment, up to 960 commercial offers may be selected from a bouquet of channels. In the Pay Per View mode, the end user is provided with the capability to purchase events as he wishes. This can be achieved

- 12 -

by either pre-booking the event in advance ("pre-book mode"), or by purchasing the event as soon as it is broadcast ("impulse mode"). In the preferred embodiment, all users are subscribers, whether or not they watch in subscription or PPV mode, but of course PPV viewers need not necessarily be subscribers.

5 Both the control word and the access criteria are used to build an Entitlement Control Message (ECM); this is a message sent in relation with one scrambled program; the message contains a control word (which allows for the descrambling of the program) and the access criteria of the broadcast program. The access criteria and control word are transmitted to the second encrypting unit 3014 via the linkage 3018. In this unit,
10 an ECM is generated, encrypted and transmitted on to the multiplexer and scrambler 2004.

Each service broadcast by a broadcast supplier in a data stream comprises a number of distinct components; for example a television programme includes a video component, an audio component, a sub-title component and so on. Each of these
15 components of a service is individually scrambled and encrypted for subsequent broadcast to the transponder 2014. In respect of each scrambled component of the service, a separate ECM is required.

Programme Transmission

The multiplexer 2004 receives electrical signals comprising encrypted EMMs from the
20 SAS 3002, encrypted ECMs from the second encrypting unit 3014 and compressed programmes from the compressor 2002. The multiplexer 2004 scrambles the programmes and transmits the scrambled programmes, the encrypted EMMs and the encrypted ECMs as electric signals to a transmitter 2008 of the broadcast centre via linkage 2010. The transmitter 2008 transmits electromagnetic signals towards the
25 satellite transponder 2014 via uplink 2012.

Programme Reception

The satellite transponder 2014 receives and processes the electromagnetic signals transmitted by the transmitter 2008 and transmits the signals on to the earth receiver

- 13 -

2018, conventionally in the form of a dish owned or rented by the end user, via downlink 2016. The signals received by receiver 2018 are transmitted to the integrated receiver/decoder 2020 owned or rented by the end user and connected to the end user's television set 2022. The receiver/decoder 2020 demultiplexes the
5 signals to obtain scrambled programmes with encrypted EMMs and encrypted ECMs.

If the programme is not scrambled, that is, no ECM has been transmitted with the MPEG-2 stream, the receiver/decoder 2020 decompresses the data and transforms the signal into a video signal for transmission to television set 2022.

If the programme is scrambled, the receiver/decoder 2020 extracts the corresponding
10 ECM from the MPEG-2 stream and passes the ECM to the "daughter" smartcard 3020 of the end user. This slots into a housing in the receiver/decoder 2020. The daughter smartcard 3020 controls whether the end user has the right to decrypt the ECM and to access the programme. If not, a negative status is passed to the receiver/decoder 2020 to indicate that the programme cannot be descrambled. If the end user does
15 have the rights, the ECM is decrypted and the control word extracted. The decoder 2020 can then descramble the programme using this control word. The MPEG-2 stream is decompressed and translated into a video signal for onward transmission to television set 2022.

Subscriber Management System (SMS)

20 A Subscriber Management System (SMS) 3004 includes a database 3024 which manages, amongst others, all of the end user files, commercial offers (such as tariffs and promotions), subscriptions, PPV details, and data regarding end user consumption and authorization. The SMS may be physically remote from the SAS.

Each SMS 3004 transmits messages to the SAS 3002 via respective linkage 3006
25 which imply modifications to or creations of Entitlement Management Messages (EMMs) to be transmitted to end users.

The SMS 3004 also transmits messages to the SAS 3002 which imply no

- 14 -

modifications or creations of EMMs but imply only a change in an end user's state (relating to the authorization granted to the end user when ordering products or to the amount that the end user will be charged).

As described later, the SAS 3002 sends messages (typically requesting information such as call-back information or billing information) to the SMS 3004, so that it will be apparent that communication between the two is two-way.

Entitlement Management Messages (EMMs)

The EMM is a message dedicated to an individual end user (subscriber), or a group of end users, only (in contrast with an ECM, which is dedicated to one scrambled programme only or a set of scrambled programmes if part of the same commercial offer). Each group may contain a given number of end users. This organisation as a group aims at optimising the bandwidth; that is, access to one group can permit the reaching of a great number of end users.

Various specific types of EMM are used in putting the present invention into practice. Individual EMMs are dedicated to individual subscribers, and are typically used in the provision of Pay Per View services; these contain the group identifier and the position of the subscriber in that group. So-called "Group" subscription EMMs are dedicated to groups of, say, 256 individual users, and are typically used in the administration of some subscription services. This EMM has a group identifier and a subscribers' group bitmap. Audience EMMs are dedicated to entire audiences, and might for example be used by a particular operator to provide certain free services. An "audience" is the totality of subscribers having smartcards which bear the same Operator Identifier (OPI). Finally, a "unique" EMM is addressed to the unique identifier of the smartcard.

The structure of a typical EMM is now described with reference to Figure 3. Basically, the EMM, which is implemented as a series of digital data bits, comprises a header 3060, the EMM proper 3062, and a signature 3064. The header 3060 in turn comprises a type identifier 3066 to identify whether the type is individual, group,

- 15 -

audience or some other type, a length identifier 3068 which gives the length of the EMM, an optional address 3070 for the EMM, an operator identifier 3072 and a key identifier 3074. The EMM proper 3062 of course varies greatly according to its type. Finally, the signature 3064, which is typically of 8 bytes long, provides a number of checks against corruption of the remaining data in the EMM.

Subscriber Authorization System (SAS)

The messages generated by the SMS 3004 are passed via linkage 3006 to the Subscriber Authorization System (SAS) 3002, which in turn generates messages acknowledging receipt of the messages generated by the SMS 3004 and passes these acknowledgements to the SMS 3004.

As shown in Figure 4, at the hardware level the SAS comprises in known fashion a mainframe computer 3050 (in the preferred embodiment a DEC machine) connected to one or more keyboards 3052 for data and command input, one or more Visual Display Units (VDUs) 3054 for display of output information and data storage means 3056. Some redundancy in hardware may be provided.

At the software level the SAS runs, in the preferred embodiment on a standard open VMS operating system, a suite of software whose architecture is now described in overview with reference to Figure 5; it will be understood that the software could alternatively be implemented in hardware.

In overview the SAS comprises a Subscription Chain area 3100 to give rights for subscription mode and to renew the rights automatically each month, a Pay Per View Chain area 3200 to give rights for PPV events, and an EMM Injector 3300 for passing EMMs created by the Subscription and PPV chain areas to the multiplexer and scrambler 2004, and hence to feed the MPEG stream with EMMs. If other rights are to be granted, such as Pay Per File (PPF) rights in the case of downloading computer software to a user's Personal Computer, other similar areas are also provided.

One function of the SAS 3002 is to manage the access rights to television

- 16 -

programmes, available as commercial offers in subscription mode or sold as PPV events according to different modes of commercialisation (pre-book mode, impulse mode). The SAS 3002, according to those rights and to information received from the SMS 3004, generates EMMs for the subscriber.

- 5 The Subscription Chain area 3100 comprises a Command Interface (CI) 3102, a Subscriber Technical Management (STM) server 3104, a Message Generator (MG) 3106, and the Cipherring Unit 3008.

- The PPV Chain area 3200 comprises an Authorisation Server (AS) 3202, a relational database 3204 for storing relevant details of the end users, a local blacklist database
10 3205, Database Servers 3206 for the database, an Order Centralized Server (OCS) 3207, a Server for Programme Broadcaster (SPB) 3208, a Message Generator (MG) 3210 whose function is basically the same as that for the Subscription Chain area and is hence not described further in any detail, and the Cipherring Unit 3008.

- The EMM Injector 3300 comprises a plurality of Message Emitters (MEs) 3302, 3304,
15 3306 and 3308 and Software Multiplexers (SMUXs) 3310 and 3312. In the preferred embodiment, there are two MEs, 3302 and 3304 for the Message Generator 3106, with the other two MEs 3306 and 3308 for the Message Generator 3210. MEs 3302 and 3306 are connected to the SMUX 3310 whilst MEs 3304 and 3308 are connected to the SMUX 3312.

- 20 Each of the three main components of the SAS (the Subscription Chain area, the PPV Chain area and the EMM Injector) are now considered in more detail.

Subscription Chain Area

- Considering first the Subscription Chain area 3100, the Command Interface 3102 is primarily for despatching messages from the SMS 3004 to the STM server 3104, as
25 well as to the OCS 3206, and from the OCS to the SMS. The Command Interface takes as input from the SMS either direct commands or batch files containing commands. It performs syntactic analysis on the messages coming from the STM

- 17 -

server, and is able to emit accurate messages when an error occurs in a message (parameter out of range, missing parameter, and so on). It traces incoming commands in textual form in a trace file 3110 and also in binary form in a replay file 3112 in order to be able to replay a series of commands. Traces can be disabled and the size of files limited.

Detailed discussion of the STM server 3104 is now provided with particular reference to Figure 6. The STM server is effectively the main engine of the Subscription Chain area, and has the purpose of managing free rights, the creation of new subscribers and the renewal of existing subscribers. As shown in the figure, commands are passed on to the Message Generator 3106, albeit in a different format from that in which the commands are passed to the STM server. For each command, the STM server is arranged to send an acknowledgement message to the CI only when the relevant command has been successfully processed and sent to the MG.

The STM server includes a subscriber database 3120, in which all the relevant parameters of the subscribers are stored (smartcard number, commercial offers, state, group and position in the group, and so on). The database performs semantic checks of the commands sent by the CI 3102 against the content of the database, and updates the database when the commands are valid.

The STM server further manages a First In First Out (FIFO) buffer 3122 between the STM server and the MG, as well as a backup disk FIFO 3124. The purpose of the FIFOs is to average the flow of commands from the CI if the MG is not able to respond for a while for any reason. They can also ensure that in the case of a crash of the STM server or MG no command will be lost, since the STM server is arranged to empty (that is, send to the MG) its FIFOs when restarted. The FIFOs are implemented as files.

The STM server includes at its core an automatic renewal server 3126 which automatically generates renewals, and, if required by the operators, free rights. In this context, the generation of renewals may be thought of as including the generation of

- 18 -

rights for the first time, although it will be understood that the generation of new rights is initiated at the SMS. As will become apparent, the two can be treated by roughly the same commands and EMMs.

Having the STM separate from the SAS, and the automatic renewal server within the SAS rather than (in known systems) in the SMS 3004, is a particularly important feature, since it can significantly reduce the number of commands which need to be passed from the SMS to the SAS (bearing in mind that the SMS and SAS may be in different locations and operated by different operators). In fact, the two main commands required from the SMS are merely commands that a new subscription should be started and that an existing subscription should be stopped (for example in the case of non-payment). By minimising command exchange between the SMS and SAS, the possibility of failure of command transfer in the linkage 3006 between the two is reduced; also, the design of the SMS does not need to take into account the features of the conditional access system 3000 generally.

Automatic renewal proceeds in the fashion indicated in the flow diagram of Figure 7. In order to reduce bandwidth, and given that a very high percentage of all renewals are standard, renewal proceeds in groups of subscribers; in the preferred embodiments there are 256 individual subscribers per group. The flow diagram begins with the start step 3130, and proceeds to step 3132 where a monthly activation of the renewal function is made (although of course it will be appreciated that other frequencies are also possible). With a monthly frequency, rights are given to the end user for the current month and all of the following month, at which point they expire if not renewed.

In step 3134 the subscriber database 3120 is accessed in respect of each group and each individual within that group to determine whether rights for the particular individual are to be renewed.

In step 3136, a group subscription bitmap is set up according to the contents of the subscriber database, as shown in Figure 8. The bitmap comprises a group identifier

- 19 -

(in this case Group 1 – "G1") 3138 and 256 individual subscriber zones 3140. The individual bits in the bitmap are set to 1 or zero according to whether or not the particular subscriber is to have his rights renewed. A typical set of binary data is shown in the figure.

- 5 In step 3142 the appropriate commands, including the group subscription bitmap, are passed to the Message Generator 3106. In step 3143 the Message Generator sets an obsolescence date to indicate to the smartcard the date beyond which the particular subscription EMM is not valid; typically this date is set as the end of the next month.

- 10 In step 3144 the Message Generator generates from the commands appropriate group subscription EMMs and asks the Ciphering Unit 3008 to cipher the EMMs, the ciphered EMMs being then passed to the EMM Injector 3300, which, in step 3146, injects the EMMs into the MPEG-2 data stream.

Step 3148 indicates that the above described procedure is repeated for each and every group. The process is finally brought to an end at stop step 3150.

- 15 The flow diagram described above with reference to Figure 7 relates in fact specifically to the renewal of subscriptions. The STM also manages in a similar way free audience rights and new subscribers.

- 20 In the case of free audience rights, available for specific television programmes or groups of such programmes, these are made available by the STM issuing a command to the Message Generator to generate appropriate audience EMMs (for a whole audience) with an obsolescence date a given number of days (or weeks) hence. The MG computes the precise obsolescence date based on the STM command.

- 25 In the case of new subscribers, these are dealt with in two stages. Firstly, on purchase the smartcard in the receiver/decoder 2020 (if desired by the operator) affords the subscriber free rights for a given period (typically a few days). This is achieved by generating a bitmap for the subscriber which includes the relevant obsolescence date.

- 20 -

The subscriber then passes his completed paperwork to the operator managing the subscriber (at the SMS). Once the paperwork has been processed, the SMS supplies to the SAS a start command for that particular subscriber. On receipt by the SAS of the start command, the STM commands the MG to assign a unique address to the new
5 subscriber (with a particular group number and position within the group) and to generate a special, so-called "commercial offer" subscription EMM (as opposed to the more usual "group" subscription EMM used for renewals) to provide the particular subscriber with rights until the end of the next month. From this point renewal of the subscriber can occur automatically as described above. By this two stage process it
10 is possible to grant new subscribers rights until the SMS issues a stop command.

It is to be noted that the commercial offer subscription EMM is used for new subscribers and for reactivation of existing subscribers. The group subscription EMM is used for renewal and suspension purposes.

With reference to Figure 9, a typical subscription EMM proper (that is, ignoring the
15 header and signature) generated by the above procedure comprises the following main portions, namely typically a 256 bit subscription (or subscribers' group) bitmap 3152, 128 bits of management ciphering keys 3154 for the ciphering of the EMM, 64 bits of each exploitation ciphering key 3156 to enable the smartcard 3020 to decipher a control word to provide access to broadcast programmes, and 16 bits of obsolescence
20 date 3158 to indicate the date beyond which the smartcard will ignore the EMM. In fact in the preferred embodiment three exploitation keys are provided, one set for the present month, one set for the next month, and one for resume purposes in the event of system failure.

In more detail, the group subscription EMM proper has all of the above components,
25 except the management ciphering keys 3154. The commercial offer subscription EMM proper (which is for an individual subscriber) includes instead of the full subscribers' group bitmap 3152 the group ID followed by the position in the group, and then management ciphering keys 3154 and three exploitation keys 3156, followed by the relevant obsolescence date 3158.

- 21 -

The Message Generator 3106 serves to transform commands issued by the STM server 3104 into EMMs for passing to the Message Emitter 3302. With reference to Figure 5, firstly, the MG produces the EMMs proper and passes them to the Ciphering Unit 3008 for ciphering with respect to the management and exploitation keys. The CU
5 completes the signature 3064 on the EMM (see Figure 3) and passes the EMM back to the MG, where the header 3060 is added. The EMMs which are passed to the Message Emitter are thus complete EMMs. The Message Generator also determines the broadcast start and stop time and the rate of emission of the EMMs, and passes these as appropriate directions along with the EMMs to the Message Emitter. The
10 MG only generates a given EMM once; it is the ME which performs its cyclic transmission.

Again with reference to Figure 5, the Message Generator includes its own EMM database 3160 which, for the lifetime of the relevant EMM, stores it. It is erased once its emission duration has expired. The database is used to ensure consistency between
15 the MG and ME, so that for example when an end user is suspended the ME will not continue to send renewals. In this regard the MG computes the relevant operations and sends them to the ME.

On generation of an EMM, the MG assigns a unique identifier to the EMM. When the MG passes the EMM to the ME, it also passes the EMM ID. This enables
20 identification of a particular EMM at both the MG and the ME.

Also concerning the Subscription Chain area, the Message Generator includes two FIFOs 3162 and 3164, one for each of the relevant Message Emitters 3302 and 3304 in the EMM Injector 3300, for storing the ciphered EMMs. Since the Subscription Chain area and EMM Injector may be a significant distance apart, the use of FIFOs
25 can allow full continuity in EMM transmission even if the links 3166 and 3168 between the two fail. Similar FIFO's are provided in the Pay Per View Chain area.

One particular feature of the Message Generator in particular and the conditional access system in general concerns the way that it reduces the length of the EMM

- 22 -

proper 3062 by mixing parameter length and identifier to save space. This is now described with reference to Figure 10 which illustrates an exemplary EMM (in fact a PPV EMM, which is the simplest EMM). The reduction in length occurs in the Pid (Packet or "Parameter" identifier) 3170. This comprises two portions, the actual ID 3172, and the length parameter for the packet 3174 (necessary in order that the start of the next packet can be identified). The whole Pid is expressed in just one byte of information, 4 bits being reserved for the ID, and four for the length. Because 4 bits is not sufficient to define the length in true binary fashion, a different correspondence between the bits and the actual length is used, this correspondence being represented in a look-up table, stored in storage area 3178 in the Message Generator (see Figure 5). The correspondence is typically as follows:-

	0000	=	0
	0001	=	1
	0010	=	2
15	0011	=	3
	0100	=	4
	0101	=	5
	0110	=	6
	0111	=	7
20	1000	=	8
	1001	=	9
	1010	=	10
	1011	=	11
	1100	=	12
25	1101	=	16
	1110	=	24
	1111	=	32

It will be seen that the length parameter is not directly proportional to the actual length of the packet; the relationship is in part more quadratic rather than linear. This allows for a greater range of packet length.

- 23 -

Pay Per View Chain Area

Concerning the Pay Per View Chain area 3200, with reference to Figure 5 in more detail the Authorisation Server 3202 has as its client the Order Centralized Server 3207, which requests information about each subscriber which connects to the
5 Communications Servers 3022 to purchase a PPV product.

If the subscriber is known from the AS 3202, a set of transactions takes place. If the subscriber is authorized for the order, the AS creates a bill and sends it to the OCS. Otherwise, it signals to the OCS that the order is not authorized.

It is only at the end of this set of transactions that the AS updates the end users
10 database 3204 via the database servers (DBAS) 3206, if at least one transaction was authorized; this optimizes the number of database accesses.

The criteria according to which the AS authorizes purchase are stored in the database, accessed through DBAS processes. In one embodiment, the database is the same as the database accessed by the STM.

15 Depending on consumer profile, the authorization may be denied (PPV_Forbidden,Casino_Forbidden ...). These kind of criteria are updated by STM 3104, on behalf of the SMS 3004.

Other parameters are checked, such as limits allowed for purchase (either by credit card, automatic payment, or number of authorized token purchases per day).

20 In case of payment with a credit card, the number of the card is checked against a local blacklist stored in the local blacklist database 3205.

When all the verifications are successful, the AS:-

1. Generates a bill and sends it to the OCS, which completes this bill and stores it in a file, this file being later sent to the SMS for processing (customer actual
25 billing); and

- 24 -

2. Updates the database, mainly to set new purchase limits.

This check-and-generate-bill-if-OK mechanism applies for each command a subscriber may request during a single connection (it is possible to order e.g. 5 movies in a single session).

- 5 It is to be noted that the AS has a reduced amount of information concerning the subscriber, by comparison with that held by the SMS. For example, the AS does not hold the name or address of the subscriber. On the other hand, the AS does hold the smartcard number of the subscriber, the subscriber's consumer category (so that different offers can be made to different subscribers), and various flags which state
10 whether, for example, the subscriber may purchase on credit, or he is suspended or his smartcard has been stolen. Use of a reduced amount of information can help to reduce the amount of time taken to authorize a particular subscriber request.

- The main purpose of the DBASs 3206 is to increase database performance seen from the AS, by paralleling the accesses (so actually it does not make much sense to define
15 a configuration with only one DBAS). An AS parameter determines how many DBASes should connect. A given DBAS may be connected to only one AS.

The OCS 2307 mainly deals with PPV commands. It operates in several modes.

- Firstly, it operates to process commands issued by the SMS, such as product refreshment (for instance, if the bill is already stored by the SMS, no bill is generated
20 by the OCS), update of the wallet in the smartcard 3020, and session cancellation/update.

The various steps in the procedure are:-

1. Identifying the relevant subscriber (using the AS 3202);
2. If valid, generate adequate commands to the Message Generator, in order to
25 send an appropriate EMM. Commands may be:

Product commands,
Update of the wallet,

- 25 -

Session erasure.

Note that these operations do not imply creation of billing information, since billing is already known from the SMS. These operations are assimilated to "free products" purchase.

- 5 Secondly, the OCS deals with commands received from the subscribers through the Communications Servers 3022. These may be received either via a modem connected to the receiver/decoder 2020, or by voice activation via the telephone 4001, or by key activation via a MINITEL, PRESTEL or like system where available.

- 10 Thirdly, the OCS deals with callback requests issued by the SMS. These last two modes of operation are now discussed in more detail.

- In the second type of mode described above it was stated that the OCS deals with commands received directly from the end user (subscriber) through the Communications Servers 3022. These include product orders (such as for a particular PPV event), a subscription modification requested by the subscriber, and a reset of a
15 parental code (a parental code being a code by which parents may restrict the right of access to certain programmes or classes of programmes).

The way in which these commands are dealt with is now described in more detail with reference to Figure 11.

Product orders by a subscriber involve the following steps:

- 20 1. Identifying through the AS the caller who is making a call through the CS 3022 ordering a particular product;
2. Checking the caller's request validity, again using the AS (where the order is placed using the receiver/decoder 2020, this is achieved by verifying the smartcard 3020 details);
- 25 3. Ascertain the price of the purchase;
4. Check that the price does not exceed the caller's credit limit etc;
5. Receiving a partial bill from the AS;

- 26 -

6. Filling additional fields in the bill to form a completed bill;
7. Adding the completed bill to a billing information storage file 3212 for later processing; and
8. Sending corresponding command(s) to the PPV Message Generator 3210 to
5 generate the relevant EMM(s).

The EMM(s) is sent either on the modem line 4002 if the consumer placed the product order using the receiver/decoder 2020 (more details of this are described later), or else it is broadcast. The one exception to this is where there is some failure of the modem connection (in the case where the consumer places the order using the
10 receiver/decoder); in this event the EMM is broadcast over the air.

A subscription modification requested by a subscriber involves:

1. Identifying the caller (using the AS);
2. Sending information to the Command Interface; the CI in turn forwards this information to the SMS; and
- 15 3. Via the CI, the OCS then receives an answer from the SMS (in terms of the cost of the modification, if the modification is possible).

If modification was requested using the receiver/decoder, the OCS generates a confirmation to the SMS. Otherwise, for example in the case of phone or Minitel, the subscriber is prompted for confirmation and this answer sent to the SMS via the OCS
20 and the CI.

Reset of a parental code involves:

1. Identifying the caller (using AS); and
2. Sending a command to the MG to generate an appropriate EMM bearing an appropriate reset password.

25 In the case of reset of parental code, the command to reset the code is for security reasons not permitted to originate from the receiver/decoder. Only the SMS, telephone and MINITEL or like can originate such a command. Hence in this

- 27 -

particular case the EMM(s) are broadcast only on air, never on the telephone line.

It will be understood from the above examples of different modes of operation of the OCS that the user can have direct access to the SAS, and in particular the OCS and AS, in that the Communications Servers are directly connected to the SAS, and in particular the OCS. This important feature is concerned with reducing the time for
5 the user to communicate his command to the SAS.

This feature is illustrated further with reference to Figure 12, from which it can be seen that the end user's Set-Top-Box, and in particular its receiver/decoder 2020, has the capability of communicating directly with the Communications Servers 3022
10 associated with the SAS 3002. Instead of the connection from the end user to the Communications Servers 3022 of the SAS 3002 being through the SMS 3004 the connection is directly to the SAS 3002.

In fact, as directly mentioned two direct connections are provided.

The first direct connection is by a voice link via a telephone 4001 and appropriate
15 telephone line (and/or by MINITEL or like connection where available) where the end users still have to input a series of voice commands or code numbers but time is saved compared with the communication being via the SMS 3004.

The second direct connection is from the receiver/decoder 2020 and the input of data is achieved automatically by the end user inserting his own daughter smartcard 3020
20 thus relieving the end user of the job of having to input the relevant data which in turn reduces the time taken and the likelihood of errors in making that input.

A further important feature which arises out of the above discussion is concerned with reducing the time taken for the resulting EMM to be transmitted to the end user in order to initiate viewing by the end user of the selected product.

25 In broad terms, and with reference to Figure 12, the feature is again achieved by

- 28 -

providing the end user's receiver/decoder 2020 with the capability of communicating directly with the Communications Servers 3022 associated with the SAS 3002.

As described earlier the integrated receiver/decoder 2020 is connected directly to the Communications Servers 3022 by the modemmed back channel 4002 so that
5 commands from the decoder 2020 are processed by the SAS 3002, messages generated (including EMMs) and then sent back directly to the decoder 2020 through the back channel 4002. A protocol is used in the communication between the CS 3022 and the receiver/decoder 2020 (as described later), so that the CS receive acknowledgement of receipt of the relevant EMM, thereby adding certainty to the procedure.

10 Thus, for example, in the case of a pre-book mode the SAS 3002 receives messages from the end user via the smartcard and decoder 2020 via its modem and via the telephone line 4002, requesting access to a specific event/product, and returns a suitable EMM via the telephone line 4002 and modem to the decoder 2020, the modem and decoder being preferably located together in a Set-Top-Box (STB). This
15 is thus achieved without having to transmit the EMM in the MPEG-2 data stream 2002 via the multiplexer and scrambler 2004, the uplink 2012, satellite 2014 and datalink 2016 to enable the end user to view the event/product. This can save considerably on time and bandwidth. Virtual certainty is provided that as soon as the subscriber has paid for his purchase the EMM will arrive at the receiver/decoder 2020.

20 In the third type of mode of operation of the OCS 3207 described above, the OCS deals with callback requests issued by the SAS. This is illustrated with reference to Figure 13. Typical callback requests have the purpose of ensuring that the receiver/decoder 2020 calls back the SAS via the modemmed back channel 4002 with the information that the SAS requires of the receiver /decoder.

25 As instructed by the Command Interface 3102, the subscription chain Message Generator 3106 generates and sends to the receiver/decoder 202 a callback EMM. This EMM is ciphered by the Ciphering Unit 3008 for security reasons. The EMM may contain the time/date at which the receiver/decoder should wake up and perform

- 29 -

a callback on its own, without being explicitly solicited; the EMM may also typically contain the phone numbers which the terminal must dial, the number of further attempts after unsuccessful calls and the delay between two calls.

When receiving the EMM, or at the specified time-date, the receiver/decoder connects
5 to the Communications Servers 3022. The OCS 3207 first identifies the caller, using the AS 3202, and verifies certain details, such as smartcard operator and subscriber details. The OCS then asks the smartcard 3020 to send various ciphered information (such as the relevant session numbers, when the session was watched, how many times the subscriber is allowed to view the session again, the way in which the session was
10 viewed, the number of remaining tokens, the number of prebooked sessions, etc). This information is deciphered by the PPV chain Message Generator 3210, again using the Ciphering Unit 3008. The OCS adds this information to a callback information storage file 3214 for later processing and passing to the SMS 3004. The information is ciphered for security reasons. The whole procedure is repeated until there is
15 nothing more to be read from the smartcard.

One particular preferred feature of the callback facility is that before reading the smartcard (so just after the identification of the caller using the AS 3202 as described above) a check is made by the SAS 3002 that the receiver/decoder is indeed a genuine one rather than a pirated version or computer simulation. Such a check is carried out
20 in the following manner. The SAS generates a random number, which is received by the receiver/decoder, ciphered, and then returned to the SAS. The SAS deciphers this number. If the deciphering is successful and the original random number is retrieved, it is concluded that the receiver/decoder is genuine, and the procedure continues. Otherwise, the procedure is discontinued.

25 Other functions which may occur during the callback are erasure of obsolete sessions on the smartcard, or filling of the wallet (this latter also being described later under the section entitled "Smartcard").

Also as regards the Pay Per View Chain area 3200, description is now made of the

- 30 -

Communications Servers 3022. At the hardware level, these comprise in the preferred embodiment a DEC Four parallel processor machine. At the software architecture level, with reference to Figure 14, in many respects the Communications Servers are conventional. One particular divergence from conventional designs arises from the fact that the Servers must serve both receiver/decoders 2020 and voice communication with conventional telephones 4001, as well possibly as MINITEL or like systems.

It will be noted in passing that two Order Centralized Servers 3207 are shown in Figure 14 (as "OCS1" and "OCS2"). Naturally any desired number may be provided.

The Communication Servers include two main servers ("CS1" and "CS2") as well as a number of frontal servers ("Frontal 1" and "Frontal 2"); whilst two frontal servers are shown in the figure, typically 10 or 12 may be provided per main server. Indeed, although two main servers CS1 and CS2 and two frontal servers, Frontal 1 and Frontal 2, have been shown, any number could be used. Some redundancy is usually desirable.

CS1 and CS2 are coupled to OCS1 and OCS2 via high level TCP/IP links 3230, whilst CS1 and CS2 are coupled to Frontal 1 and Frontal 2 via further TCP/IP links 3232.

As illustrated, CS1 and CS2 comprise servers for "SENDER" (transmission), "RECEIVER" (reception), "VTX" (MINITEL, PRESTEL or the like), "VOX" (voice communication), and "TRM" (communication with the receiver/decoder). These are coupled to the "BUS" for communication of signals to the Frontal servers.

CS1 and CS2 communicate directly with the receiver/decoders 2020 via their modemmed back channels 4002 using the X25 public network common protocol. The relatively low-level protocol between the Communications Servers 3022 and the receiver/decoders 3020 is in one preferred embodiment based upon the V42 standard international CCITT protocol, which provides reliability by having error detection and data re-transmission facilities, and uses a checksum routine to check the integrity of

- 31 -

the re-transmission. An escape mechanism is also provided in order to prevent the transmission of disallowed characters.

On the other hand, voice telephone communication is carried out via the Frontal Communications Servers, each capable of picking up, say, 30 simultaneous voice
5 connections from the connection 3234 to the local telephone network via the high speed "T2" (E1) standard telephony ISDN lines.

Three particular functions of the software portion of the Communications Servers (which could of course alternatively be implemented fully in hardware) are firstly to convert the relatively low level protocol information received from the
10 receiver/decoder into the relatively high level protocol information output to the OCS, secondly to attenuate or control the number of simultaneous connections being made, and thirdly to provide several simultaneous channels without any mixing. In this last regard, the Communications Servers play the role of a form of multiplexer, with the interactions in a particular channel being defined by a given Session ID (identifier),
15 which is in fact used throughout the communication chain.

Finally as regards the Pay Per View Chain area 3200, and with reference again to Figure 5, the Server for Programme Broadcast (SPB) 3208 is coupled to one or more Programme Broadcasters 3250 (which would typically be located remotely from the SAS) to receive programme information. The SPB filters out for further use
20 information corresponding to PPV events (sessions).

A particularly important feature is that the filtered programme event information is passed by the SPB to the MG which in turn sends a directive (control command) to the ME to change the rate of cyclic emission of the EMMs in given circumstances; this is done by the ME finding all EMMs with the relevant session identifier and
25 changing the cycle rate allocated to such EMMs. This feature might be thought of as a dynamic allocation of bandwidth for specific EMMs. Cyclic EMM emission is discussed in more detail in the section below concerned with the EMM Injector.

- 32 -

The circumstances in which the cycle rate is changed are now described with reference to Figure 15, which demonstrates how cycle rate 3252 is raised a short while (say 10 minutes) before a particular PPV programme event until the end of the event from a slow cycle rate of say once every 30 minutes to a fast cycle rate of say once every 30 seconds to 1 minute in order to meet the anticipated extra user demand for PPV events at those times. In this way bandwidth can be allocated dynamically according to the anticipated user demand. This can assist in reducing the overall bandwidth requirement.

The cycle rate of other EMMs may also be varied. For example the cycle rate of subscription EMMs may be varied by the Multiplexer and Scrambler 2004 sending the appropriate bitrate directive.

EMM Injector

Concerning the EMM Injector 3300, details of the Message Emitters 3302 to 3308, forming part of the EMM Injector and acting as output means for the Message Generator, are now described with reference to Figure 16. Their function is take the EMMs and to pass them cyclically (in the manner of a carousel) via respective links 3314 and 3316 to the Software Multiplexers 3310 and 3312 and thence to the hardware multiplexers and scramblers 2004. In return the software multiplexers and scramblers 2004 generate a global bitrate directive to control the overall cycling rate of the EMMs; to do so, the MEs take into account various parameters such as the cycle time, the size of EMM, and so on. In the figure, EMM_X and EMM_Y are group EMMs for operators X and Y, whilst EMM_Z are other EMMs for either operator X or operator Y.

Further description proceeds for an exemplary one of the Message Emitters; it will be appreciated that the remaining MEs operate in similar fashion. The ME operates under control of directives from the MG, most notably transmission start and stop time and emission rate, as well as session number if the EMM is a PPV EMM. In relation to the emission rate, in the preferred embodiment the relevant directive may take one of five values from Very fast to Very slow. The numeric values are not specified in

- 33 -

the directive, but rather the ME maps the directive to an actual numeric value which is supplied by the relevant part of the SAS. In the preferred embodiment, the 5 emission rates are as follows:-

- | | | | |
|---|----|-----------|--------------------|
| 5 | 1. | Very fast | - every 30 seconds |
| | 2. | Fast | - every minute |
| | 3. | Medium | - every 15 minutes |
| | 4. | Slow | - every 30 minutes |
| | 5. | Very slow | - every 30 minutes |

10 The ME has first and second databases 3320 and 3322. The first database is for those EMMs which have not yet achieved their broadcast date; these are stored in a series of chronological files in the database. The second database is for EMMs for immediate broadcast. In the event of a system crash, the ME is arranged to have the ability to re-read the relevant stored file and perform correct broadcast. All the files stored in the databases are updated upon request from the MG, when the MG wishes 15 to maintain consistency between incoming directives and EMMs already sent to the ME. The EMMs actually being broadcast are also stored in Random Access Memory 3324.

20 A combination of the FIFOs 3162 and 3164 in the Message Generator and the databases 3320 and 3322 in the Message Emitter means that the two can operate in standalone mode if the link 3166 between them is temporarily broken; the ME can still broadcast EMMs.

25 The Software Multiplexers (SMUX) 3310 and 3312 provide an interface between the MEs and the hardware multiplexers 2004. In the preferred embodiment, they each receive EMMs from two of the MEs, although in general there is no restriction on the number of MEs that can be connected with one SMUX. The SMUXs concentrate the EMMs and then pass them according to the type of EMM to the appropriate hardware multiplexer. This is necessary because the hardware multiplexers take the different types of EMMs and place them at different places in the MPEG-2 stream. The

- 34 -

SMUX's also forward global bitrate directives from the hardware multiplexers to the MEs.

One particularly important feature of the ME is that it emits EMMs in random order. The reason for this is as follows. The Message Emitter has no ability to sense or
5 control what it emits to the multiplexer. Hence it is possible that it may transmit two EMMs which are to be received and decoded by the receiver/decoder 2020 back to back. In such circumstances, further, it is possible that if the EMMs are insufficiently separated the receiver/decoder and smartcard will be unable to sense and decode properly the second of the EMMs. Cyclically emitting the EMMs in random order
10 can solve this problem.

The manner in which randomization is achieved is now described with reference to Figure 17; in the preferred embodiment the necessary software logic is implemented in the ADA computer language. A particularly important part of the randomization is the correct storage of the EMMs in the databases 3320 and 3322 (which are used
15 for backup purposes) and in the RAM 3324. For a particular cycle rate and operator, the EMMs are stored in a two-dimensional array, by rank 3330 (going say from A to Z) and number in the rank 3332 (going from 0 to N). A third dimension is added by cycle rate 3334, so that there are as many two-dimensional arrays as there are cycle rates. In the preferred embodiment there are 256 ranks and typically 200 or 300
20 EMMs in each rank; there are 5 cycle rates. A final dimension to the array is added by the presence of different operators; there are as many three-dimensional arrays as there are operators. Storage of the data in this fashion can permit rapid retrieval in the event that the MG wants to delete a particular EMM.

Storage of the EMMs takes place according to the "hash" algorithm (otherwise known
25 as the "one-way hash function". This operates on a modulo approach, so that successive ranks are filled before a higher number in the rank is used, and the number of EMMs in each rank remains roughly constant. The example is considered of there being 256 ranks. When the MG sends the ME an EMM with identifier (ID) 1, the rank "1" is assigned to this EMM, and it takes the first number 3332 in the rank 3330.

- 35 -

The EMM with ID 2 is assigned the rank "2", and so on, up to the rank 256. The EMM with ID 257 is assigned the rank "1" again (based on the modulo function), and takes the second number in the first rank, and so on.

5 Retrieval of a specific EMM, for example when deletion of a specific EMM is requested by the MG, is effected by means of the inverse of the above. The hash algorithm is applied to the EMM ID to obtain the rank, after which the number in the rank is found.

10 The actual randomization occurs when the EMMs are, on a cyclical basis, retrieved from RAM 3324 using the randomization means 3340 which is implemented in the hardware and/or software of the Message Emitter. The retrieval is random, and again based on the hash algorithm. Firstly, a random number (in the above example initially in the range 1 to 256) is chosen, to yield the particular rank of interest. Secondly, a further random number is chosen to yield the particular number in the rank. The further random number is selected according to the total number of EMMs in a given rank. Once a given EMM has been selected and broadcast, it is moved to a second identical storage area in the RAM 3324, again using the hash function. Hence the first area diminishes in size as the EMMs are broadcast, to the extent that, once a complete rank has been used, this is deleted. Once the first storage area is completely empty, it is replaced by the second storage area before a new round of EMM broadcast, and vice versa.

15

20

In the above fashion, after two or three cycles of the EMMs, statistically the chances of any two EMMs destined for the same end user being transmitted back to back is negligible.

25 At regular intervals whilst the EMMs are being stored the computer 3050 computes the number of bytes in storage and from this computes the bitrate of emission given the global bitrate directive from the multiplexer and software multiplexer.

Reference was made above to the backup databases 3320 and 3322. These are in fact

- 36 -

in the preferred embodiment sequential file stores, which hold a backup version of what is in the RAM 3324. In the event of failure of the Message Emitter and subsequent restart, or more generally when the ME is being restarted for whatever reason, a link is made between the RAM and the databases, over which the stored
5 EMMs are uploaded to RAM. In this way, the risk of losing EMMs in the event of failure can be removed.

Similar storage of PPV EMMs occurs to that described above in relation to subscription EMMs, with the rank typically corresponding to a given operator and the number in the rank corresponding to the session number.

10 Smartcard

A daughter, or "subscriber", smartcard 3020 is schematically shown in Figure 18 and comprises an 8 bit microprocessor 110, such as a Motorola 6805 microprocessor, having an input/output bus coupled to a standard array of contacts 120 which in use are connected to a corresponding array of contacts in the card reader of the
15 receiver/decoder 2020, the card reader being of conventional design. The microprocessor 110 is also provided with bus connections to preferably masked ROM 130, RAM 140 and EEPROM 150. The smartcard complies with the ISO 7816-1, 7816-2 and 7816-3 standard protocols which determine certain physical parameters of the smartcard, the positions of the contacts on the chip and certain communications
20 between the external system (and particularly the receiver/decoder 2020) and the smartcard respectively and which will therefore not be further described here. One function of the microprocessor 110 is to manage the memory in the smartcard, as now described.

The EEPROM 150 contains certain dynamically-created operator zones 154, 155, 156
25 and dynamically-created data zones which will now be described with reference to Figure 19.

Referring to Figure 19, EEPROM 150 comprises a permanent "card ID" (or manufacturer) zone 151 of 8 bytes which contains a permanent subscriber smartcard

- 37 -

identifier set by the manufacturer of the smartcard 3020.

When the smartcard is reset, the microprocessor 110 issues a signal to receiver/decoder 2020, the signal comprising an identifier of the conditional access system used by the smartcard and data generated from data stored in the smartcard, including the card ID. This signal is stored by the receiver/decoder 2020, which subsequently utilises the stored signal to check whether the smartcard is compatible with the conditional access system used by the receiver/decoder 2020.

The EEPROM 150 also contains a permanent "random number generator" zone 152 which contains a program for generating pseudo-random numbers. Such random numbers are used for diversifying transaction output signals generated by the smartcard 3020 and sent back to the broadcaster.

Below the random number generator zone 152 a permanent "management" zone 153 of 144 bytes is provided. The permanent management zone 153 is a specific operator zone utilised by a program in the ROM 130 in the dynamic creation (and removal) of zones 154, 155, 156... as described below. The permanent management zone 153 contains data relating to the rights of the smartcard to create or remove zones.

The program for dynamically creating and removing zones is responsive to specific zone creation (or removal) EMMs which are transmitted by the SAS 3002 and received by the receiver/decoder 2020 and passed to the subscriber smartcard 3020. In order to create the EMMs the operator requires specific keys dedicated to the management zone. This prevents one operator from deleting zones relating to another operator.

Below the management zone 153 is a series of "operator ID" zones 154, 155, 156 for operators 1, 2 N respectively. Normally at least one operator ID zone will be preloaded into the EEPROM of the subscriber smartcard 3020 so that the end user can decrypt programmes broadcast by that operator. However further operator ID zones can subsequently be dynamically created using the management zone 153 in response

- 38 -

to a transaction output signal generated via his smartcard 3020 by the end user (subscriber), as will subsequently be described.

Each operator zone 154, 155, 156 contains the identifier of the group to which the smartcard 3020 belongs, and the position of the smartcard within the group. This data enables the smartcard (along with the other smartcards in its group) to be responsive to a broadcast "group" subscription EMM having that group's address (but not the smartcard's position in the group) as well as to an "individual" (or commercial offers subscription) EMM addressed only to that smartcard within the group. There can be 256 member smartcards of each such group and this feature therefore reduces significantly the bandwidth required for broadcasting EMMs.

In order to reduce further the bandwidth required for broadcasting "group" subscription EMMs, the group data in each operator zone 154, 155, 156 and all similar zones in the EEPROM of smartcard 3020 and the other daughter smartcards is continually updated to enable a particular smartcard to change its position in each group to fill any holes created by e.g. deletion of a member of the group. The holes are filled by the SAS 3002 as in the STM server 3104 there is a list of such holes.

In this manner fragmentation is reduced and each group's membership is maintained at or near the maximum of 256 members.

Each operator zone 154, 155, 156 is associated with one or more "operator data objects" stored in the EEPROM 150. As shown in Figure 19, a series of dynamically created "operator data" objects 157-165 are located below the operator ID zones. Each of these objects is labelled with:

- a) an "identifier" 1, 2, 3 N corresponding to its associated operator 1, 2, 3 ... N as shown in its left hand section in Figure 19;
- b) an "ID" indicating the type of object; and
- c) a "data" zone reserved for data, as shown in the right hand section of each relevant operator object in Figure 19. It should be understood that each operator is associated with a similar set of data objects so that the following description of the

- 39 -

types of data in the data objects of operator 1 is also applicable to the data objects of all the other operators. Also it will be noted that the data objects are located in contiguous physical regions of the EEPROM and that their order is immaterial.

5 Deletion of a data object creates a "hole" 166 in the smartcard, that is, the number of bytes that the deleted objects had previously occupied are not immediately occupied. The thus "freed" number of bytes, or "hole" are labelled with:

- a) an "identifier" 0; and
- b) an "ID" indicating that the bytes are free to receive an object.

10 The next data object created fills the hole, as identified by the identifier 0. In this manner the limited memory capacity (4 kilobytes) of the EEPROM 150 is efficiently utilised.

Turning now to the set of data objects associated with each operator, examples of the data objects are now described.

15 Data object 157 contains an EMM key used for decrypting encrypted EMM's received by the receiver/decoder 2020. This EMM key is permanently stored in the data object 157. This data object 157 may be created prior to distribution of the smartcard 3020, and/or may be created dynamically when creating a new operator zone (as described above).

20 Data object 159 contains ECM keys which are sent by the associated operator (in this case operator 1) to enable the end user to decrypt the particular "bouquet" of programs to which he has subscribed. New ECM keys are sent typically every month, along with a group subscription (renewal) EMM which renews the end user's overall right to view the broadcast from (in this case) operator 1. The use of separate EMM and ECM keys enables viewing rights to be purchased in different ways (in this
25 embodiment by subscription and individually (Pay Per View)) and also increases security. The Pay Per View (PPV) mode will be described subsequently.

- 40 -

Since new ECM keys are sent periodically, it is essential to prevent a user from using old ECM keys, for example by switching off the receiver/decoder or re-setting a clock to prevent expiry of an old ECM key so that a timer in the receiver/decoder 2020 could be overridden. Accordingly operator zone 154 comprises an area (typically
5 having a size of 2 bytes) containing an obsolescence date of the ECM keys. The smartcard 3020 is arranged to compare this date with the current date which is contained in received ECMs and to prevent decryption if the current date is later than the obsolescence date. The obsolescence date is transmitted via EMMs, as described above.

10 Data object 161 contains a 64 bit subscription bitmap which is an exact representation of the broadcast operator's programs to which the subscriber has subscribed. Every bit represents a program and is set to "1" if it is subscribed to and "0" if it is not.

Data object 163 contains a quantity of tokens which can be used by the consumer in PPV mode to buy viewing rights to an imminent broadcast e.g. in response to a free
15 preview or other advertisement. Data object 163 also contains a limit value, which may be set to e.g. a negative value to allow credit to the consumer. Tokens can be purchased e.g. by credit and via the modemmed back channel 4002, or by using a voice server in combination with a credit card, for example. A particular event can be charged as one token or a number of tokens.

20 Data object 165 contains a description of a PPV event, as shown with reference to table 167 of Figure 20.

The PPV event description 167 contains a "session ID" 168 identifying the viewing session (corresponding to the program and the time and date of broadcasting) a
"session mode" 169 indicating how the viewing right is being purchased (e.g. in pre-
25 book mode), a "session index" 170 and a "session view" 171.

In respect of receiving a programme in PPV mode, the receiver decoder 2020 determines whether the programme is one sold in PPV mode. If so, the decoder 2020

- 41 -

checks, using the items stored in the PPV event description 167 whether the session ID for the programme is stored therein. If the session ID is stored therein, the control word is extracted from the ECM.

5 If the session ID is not stored therein, by means of a specific application the receiver/decoder 2020 displays a message to the end user indicating that he has the right to view the session at a cost of, say, 25 tokens, as read from the ECM or to connect to the communications servers 3022 to purchase the event. Using the tokens, if the end user answers "yes" (by means of remote controller 2026 (see Figure 2)) the decoder 2020 sends the ECM to the smartcard, the smartcard decreases the wallet of
10 the smartcard 3020 by 25 tokens, writes the session ID 168, the session mode 169, the session index 170 and the session view 171 in the PPV event description 167 and extracts and deciphers the control word from the ECM.

In the "pre-book" mode, an EMM will be passed to the smartcard 3020 so that the smartcard will write the session ID 168, the session mode 169, the session index 170
15 and the session view 171 in the PPV event description 167 using the EMM.

*Pre-Book
more*

The session index 170 can be set to differentiate one broadcast from the other. This feature permits authorization to be given for a subset of broadcasts, for example, 3 times out of 5 broadcasts. As soon as an ECM with a session index different from the current session index 170 stored in the PPV event description 167 is passed to the
20 smartcard, the number of the session view 171 is decreased by one. When the session view reaches zero, the smartcard will refuse to decipher an ECM with a different session index to the current session index.

The initial value of the session view depends only on the way in which the broadcast supplier wishes to define the event to which it relates; the session view for a
25 respective event may take any value.

The microprocessor 110 in the smartcard implements a counting and a comparison program to detect when the limit to the number of viewings of a particular program

- 42 -

has been reached.

All of the session ID 168, the session mode 169, the session index 170 and the session view 171 in the PPV event description 167 may be extracted from the smartcard using the "call-back" procedure as described previously.

- 5 Each receiver/decoder 2020 contains an identifier which may either identify uniquely that receiver/decoder or identify its manufacturer or may classify it in some other way in order to enable it to work only with a particular individual smartcard, a particular class of smartcards made by the same or a corresponding manufacturer or any other class of smartcards which are intended for use with that class of receiver/decoders
10 exclusively.

In this manner the receiver/decoders 2020 which have been supplied by one broadcast supplier to the consumer are protected against the use of non-authorised daughter smartcards 3020.

- 15 Additionally or alternatively to this first "handshake" between the smartcard and the receiver, the EEPROM of the smartcard 3020 could contain a field or bitmap describing the categories of receiver/decoders 2020 with which it can function. These could be specified either during the manufacture of the smartcard 3020 or by a specific EMM.

- 20 The bitmap stored in the smartcard 3020 typically comprises a list of up to 80 receiver/decoders, each identified with a corresponding receiver/decoder ID with which the smartcard may be used. Associated with each receiver/decoder is a level "1" or "0" indicating whether the smartcard may be used with the receiver/decoder or not, respectively. A program in the memory 2024 of the receiver/decoder searches for the identifier of the receiver/decoder in the bitmap stored in the smartcard. If the
25 identifier is found, and the value associated with the identifier is "1", then the smartcard is "enabled"; if not, then the smartcard will not function with that receiver/decoder.

- 43 -

In addition, if, typically because of an agreement between operators, it is desired to authorize the use of other smartcards in a particular receiver/decoder, specific EMMs will be sent to those smartcards to change their bitmap via the transponder 2014.

Each broadcast supplier may differentiate his subscribers according to certain
5 predetermined criteria. For example, a number of subscribers may be classed as "VIPs". Accordingly, each broadcast supplier may divide his subscribers into a plurality of subsets, each subset comprising any number of subscribers.

The subset to which a particular subscriber belongs is set in the SMS 3004. In turn, the SAS 3002 transmits an EMM to the subscriber which writes information (typically
10 of length 1 byte) concerning the subset to which the subscriber belongs into the relevant operator data zone, say 154, of the EEPROM of the smartcard. In turn, as events are broadcast by the broadcast supplier, an ECM, typically of 256 bits, is transmitted with the event and indicating which of the subsets of subscribers may view the event. If, according to the information stored in the operator zone, the subscriber
15 does not have the right to view the event, as determined by the ECM, programme viewing is denied.

This facility may be used, for example, to switch off all of a given operator's smartcards in a particular geographical region during the transmission of a particular program, in particular a program relating to a sports fixture taking place in that
20 geographical region. In this manner football clubs and other sport bodies can sell broadcasting rights outside their locality whilst preventing local supporters from viewing the fixture on television. In this manner the local supporters are encouraged to buy tickets and attend the fixture.

Each of the features associated with zones 151 to 172 is considered to be a separate
25 invention independent of the dynamic creation of zones.

It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the

- 44 -

invention.

Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

In the aforementioned preferred embodiments, certain features of the present invention have been implemented using computer software. However, it will of course be clear to the skilled man that any of these features may be implemented using hardware. Furthermore, it will be readily understood that the functions performed by the hardware, the computer software, and such like are performed on or using electrical and like signals.

10 Cross reference is made to our co-pending applications, all bearing the same filing date, and entitled Signal Generation and Broadcasting (Attorney Reference no. PC/ASB/19707), Smartcard for use with a Receiver of Encrypted Broadcast Signals, and Receiver (Attorney Reference No. PC/ASB/19708), Broadcast and Reception System and Conditional Access System therefor (Attorney Reference No. 15 PC/ASB/19710), Downloading a Computer File from a Transmitter via a Receiver/Decoder to a Computer (Attorney Reference No. PC/ASB/19711), Transmission and Reception of Television Programmes and Other Data (Attorney Reference No. PC/ASB/19712), Downloading Data (Attorney Reference No. PC/ASB/19713), Computer Memory Organisation (Attorney Reference No. 20 PC/ASB/19714), Television or Radio Control System Development (Attorney Reference No. PC/ASB/19715), Extracting Data Sections from a Transmitted Data Stream (Attorney Reference No. PC/ASB/19716), Access Control System (Attorney Reference No. PC/ASB/19717), Data Processing System (Attorney Reference No. PC/ASB/19718), and Broadcast and Reception System, and Receiver/Decoder and 25 Remote Controller therefor (Attorney Reference No. PC/ASB/19720). The disclosures of these documents are incorporated herein by reference. The list of applications includes the present application.

- 45 -

CLAIMS

1. A conditional access system comprising:
means for generating a plurality of messages; and
means for receiving the messages, said receiving means being adapted to
5 communicate with said generating means via a communications server connected
directly to said generating means.
2. A conditional access system according to Claim 1, wherein said message is an
entitlement message for transmission to the receiving means, said generating means
being adapted to generate entitlement messages in response to data received from said
10 receiving means.
3. A conditional access system according to Claim 1 or 2, wherein said generating
means is arranged to transmit a message as a packet of digital data to said receiving
means either via said communications server or via a satellite transponder.
4. A conditional access system according to any preceding claim, wherein said
15 receiving means is connectable to said communications server via a modem and
telephone link.
5. A conditional access system for affording conditional access to subscribers,
comprising:
a subscriber management system;
20 a subscriber authorization system coupled to the subscriber management
system; and
a communications server; said server being connected directly to the subscriber
authorization system.
6. A conditional access system according to Claim 5, further comprising a
25 receiver/decoder for the subscriber, the receiver/decoder being connectable to said
communications server, and hence to said subscriber authorization system, via a

- 46 -

modem and telephone link.

7. A broadcast and reception system including a conditional access system according to any preceding claim.

8. A broadcast and reception system comprising:

5 means for generating a plurality of entitlement messages relating to broadcast programs;

means for receiving said messages from said generating means; and

means for connecting the receiving means to the generating means to receive said messages, said connecting means being capable of effecting a dedicated
10 connection between the receiving means and the generating means.

9. A broadcast and reception system comprising:

means for generating a plurality of entitlement messages relating to broadcast programs;

15 means for receiving said messages from said generating means via a modem;

and

means for connecting said modem to said generating means and said receiving means.

10. A broadcast and reception system according to Claim 9, wherein said generating means is connected to said modem via a communications server.

20 11. A broadcast and reception system according to Claim 9 or 10, wherein said receiving means is adapted to communicate with said generating means via said modem and connecting means.

12. A broadcast and reception system according to Claim 11, wherein said receiving means comprises means for reading a smartcard insertable therein by an
25 end user, the smartcard having stored therein data to initiate automatically the transmission of a message from said receiving means to said generating means upon

- 47 -

insertion of the smartcard by the end user.

13. A broadcast and reception system according to Claim 11 or 12, further comprising a voice link to enable the end user of the broadcast and reception system to communicate with the generating means.

5 14. A broadcast and reception system according to any of Claims 8 to 13, wherein said receiving means comprises a receiver/decoder comprising means for receiving a compressed MPEG-type signal, means for decoding the received signal to provide a television signal and means for supplying the television signal to a television.

10 15. A broadcast and reception system, comprising, at the broadcast end:
a broadcast system including means for broadcasting a callback request;
and at the reception end:
a receiver including means for calling back the broadcast system in response to the callback request.

15 16. A system according to Claim 15, wherein the means for calling back the broadcast system includes a modem connectable to a telephone system.

17. A system according to Claim 15 or 16, wherein the means for calling back the broadcast system is arranged to transfer to the broadcast system information concerning the receiver.

20 18. A system according to Claim 17, wherein the broadcast system includes means for storing the information.

19. A system according to any of Claims 15 to 18, wherein the broadcast means is arranged to broadcast a callback request which includes a command that the callback be made at a given time, and the means for calling back the broadcast system is arranged to respond to said command.

- 48 -

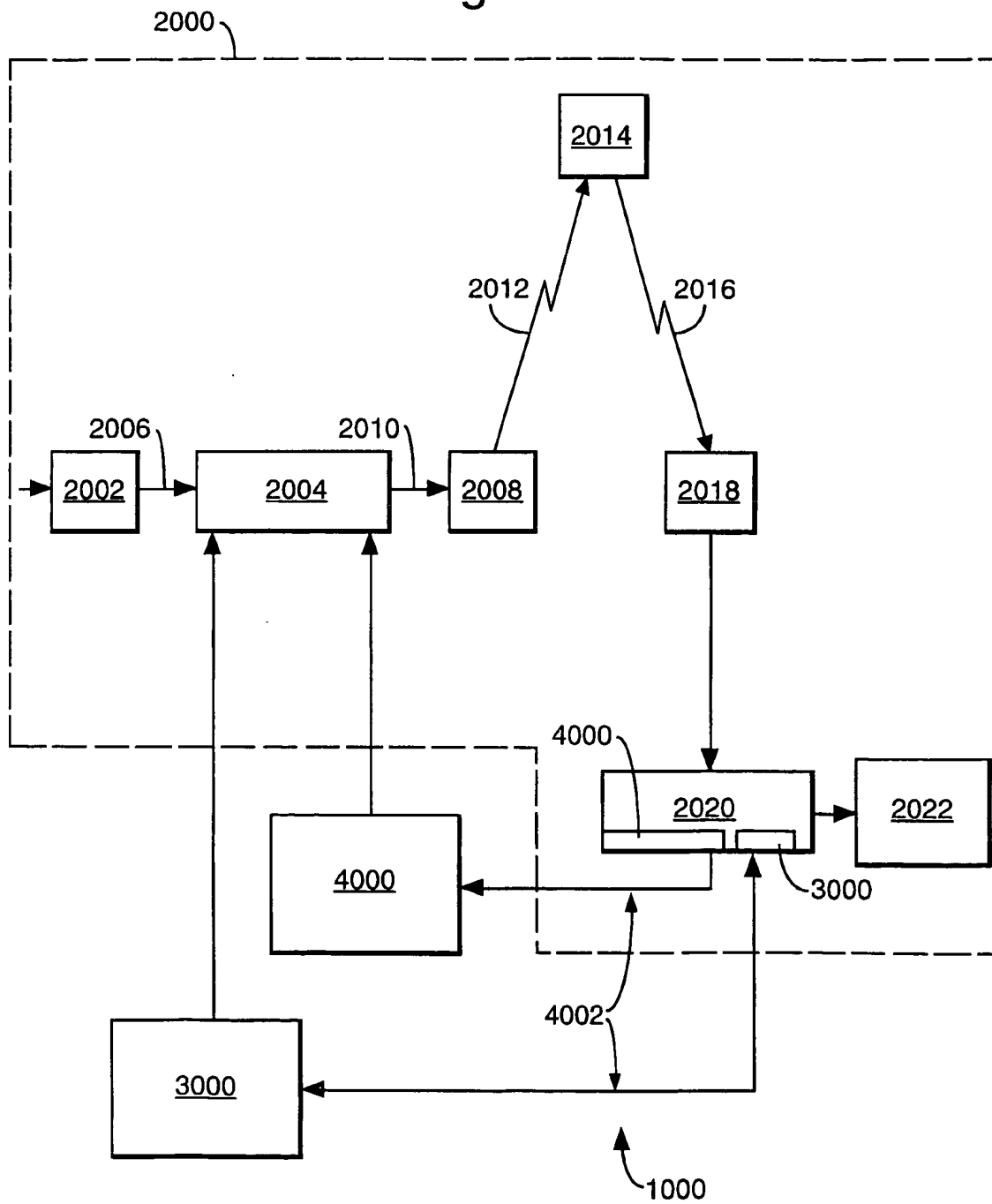
20. A system according to any of Claims 15 to 19, wherein the broadcasting means is arranged to broadcast as the callback request one or more entitlement messages for broadcast.

5 21. A system according to any of Claims 15 to 20, wherein the broadcast system includes means for generating a check message and passing this to the receiver, the receiver includes means for encrypting the check message and passing this to the broadcast system, and the broadcast system further includes means for decrypting the check message received from the receiver and comparing this with the original check message.

10 22. A conditional access system or a broadcast and reception system substantially as herein described with reference to and as illustrated in the accompanying drawings, and especially Figures 12, 13 or 14 thereof.

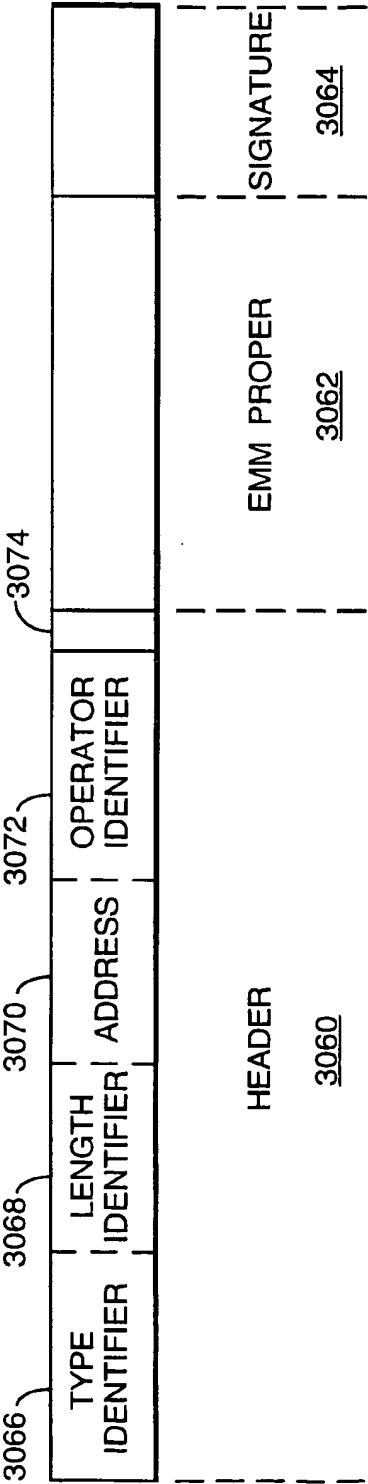
1/17

Fig.1.

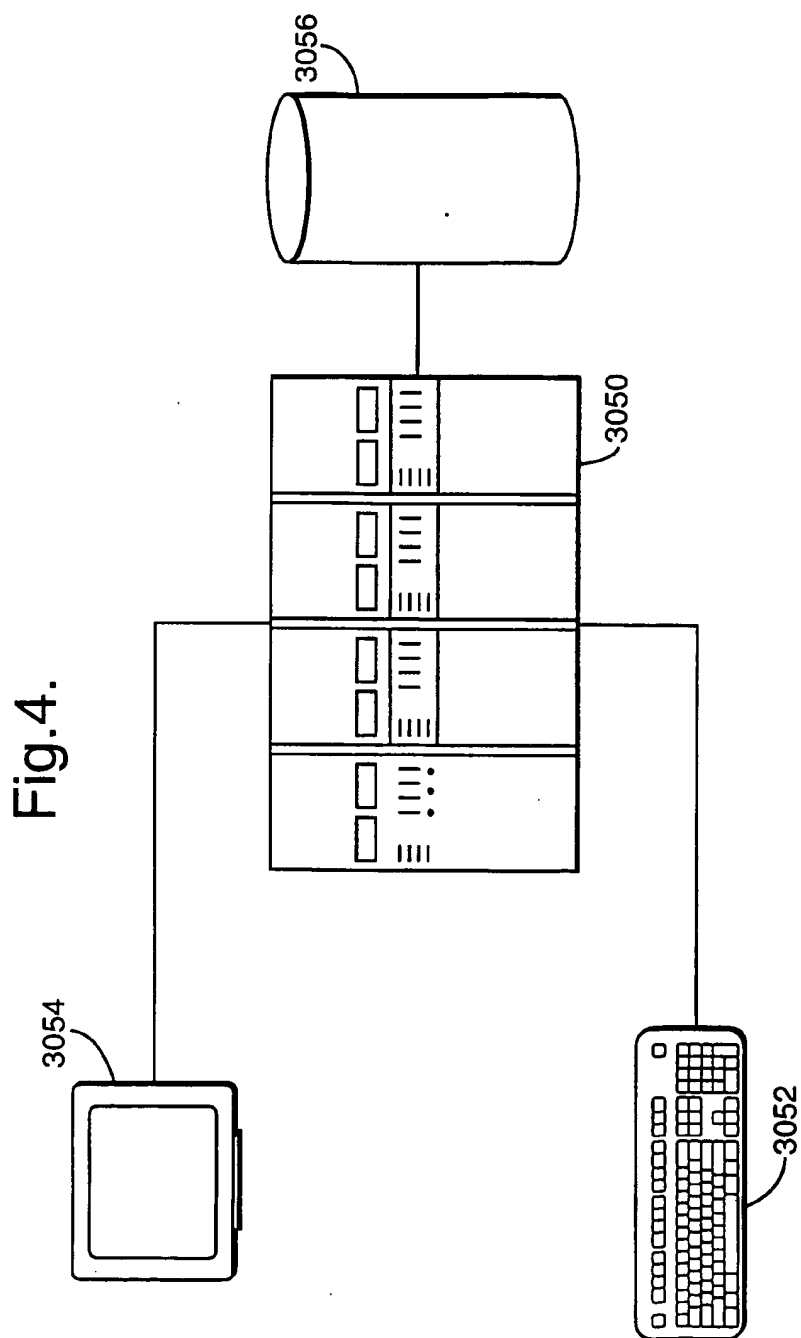


SUBSTITUTE SHEET (RULE 26)

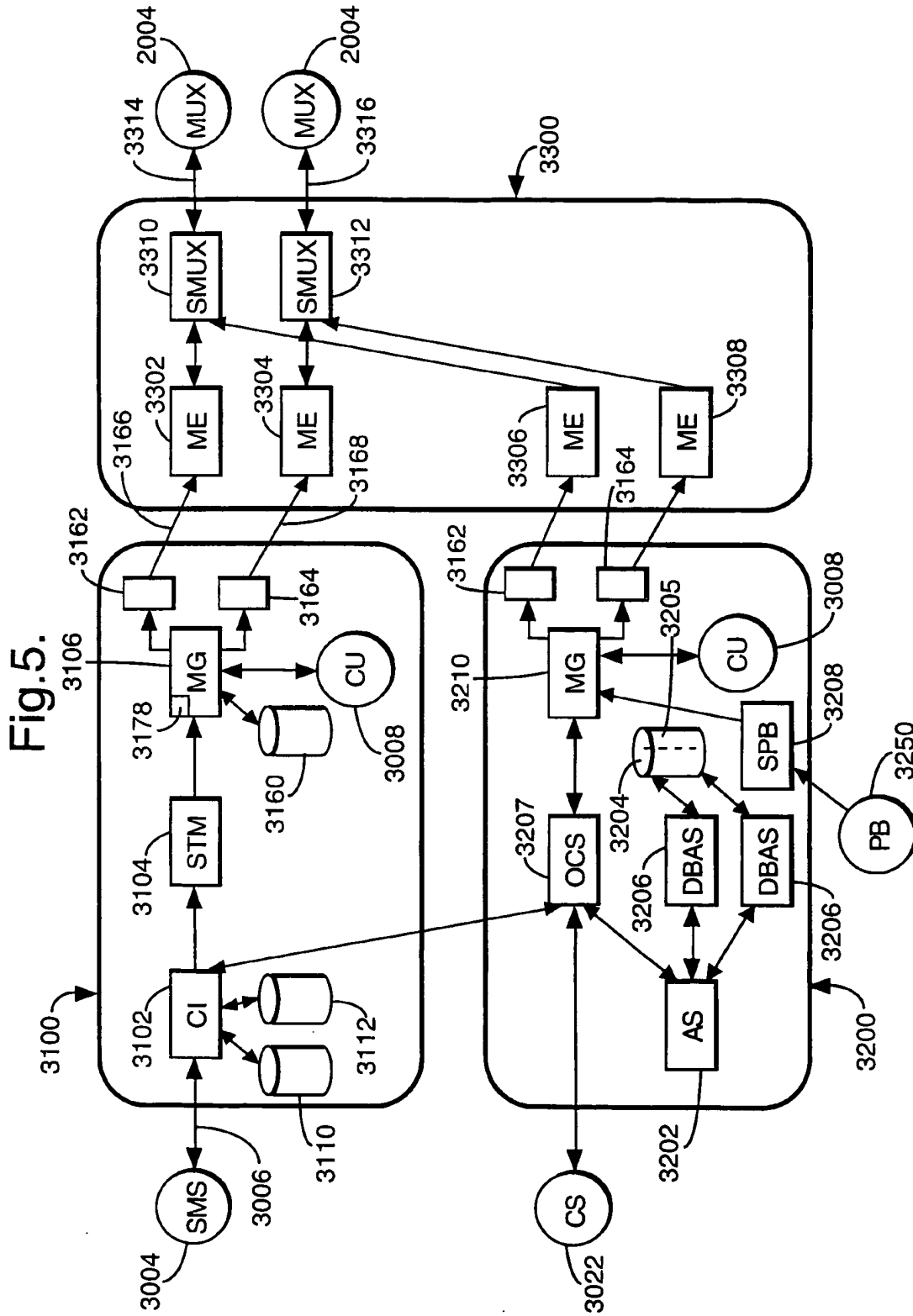
Fig.3.



4/17

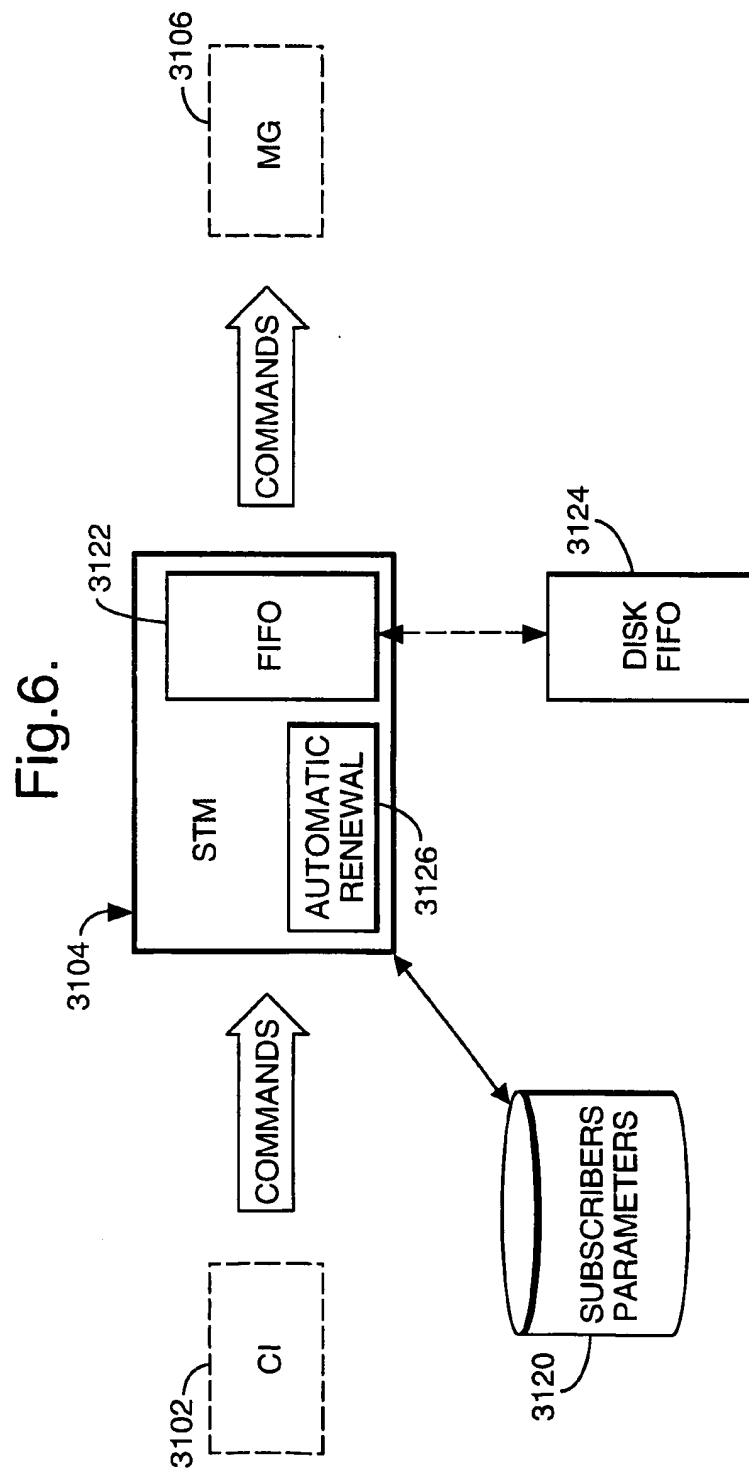


SUBSTITUTE SHEET (RULE 26)



SUBSTITUTE SHEET (RULE 26)

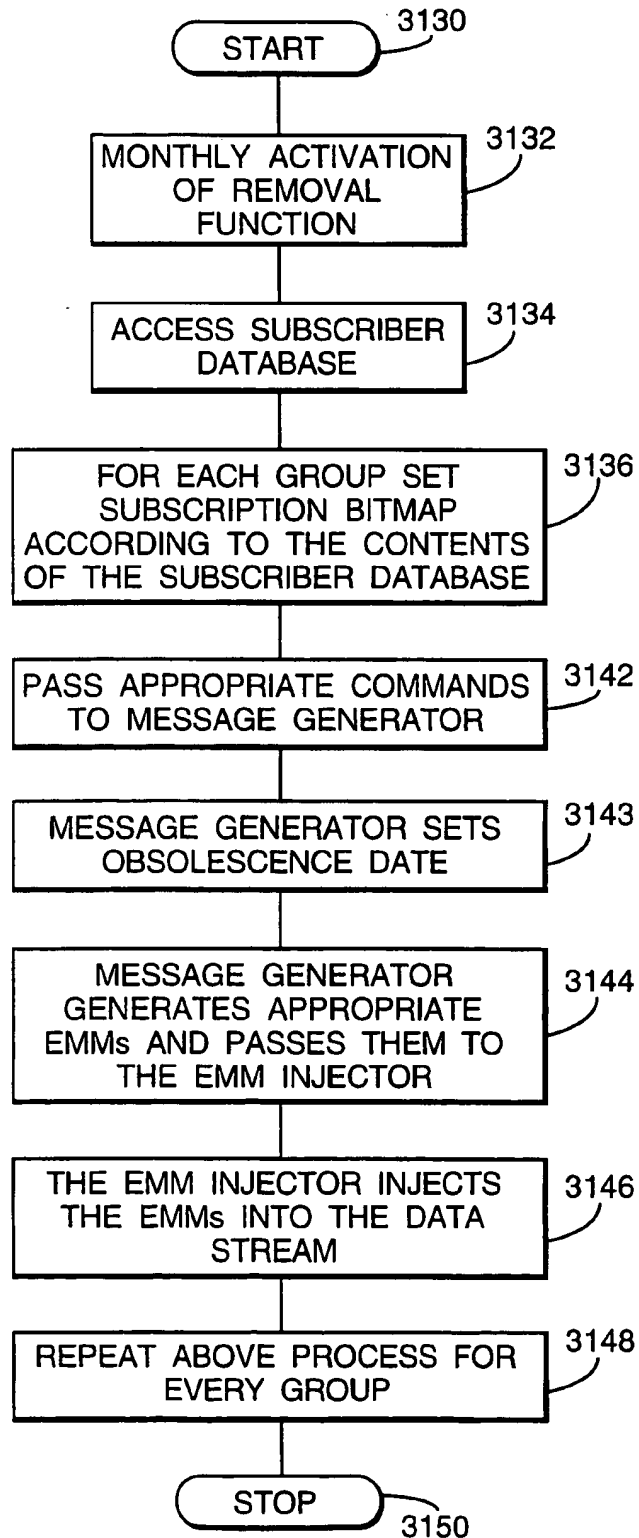
6/17



SUBSTITUTE SHEET (RULE 26)

7/17

Fig.7.



SUBSTITUTE SHEET (RULE 26)

8/17

Fig.8.

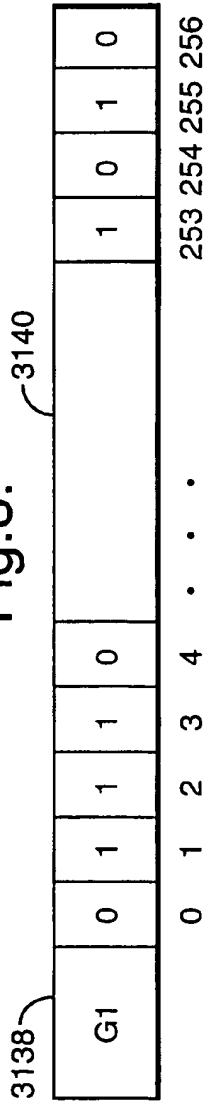


Fig.9.

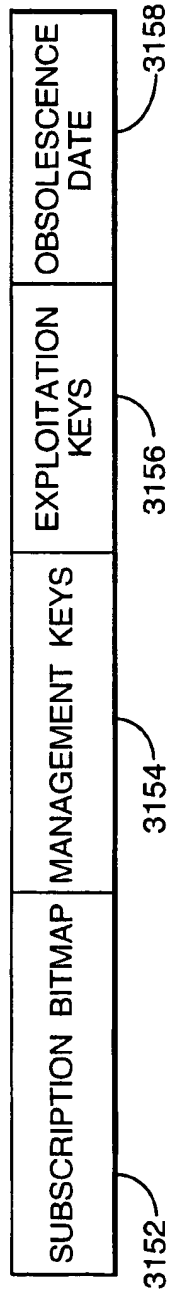
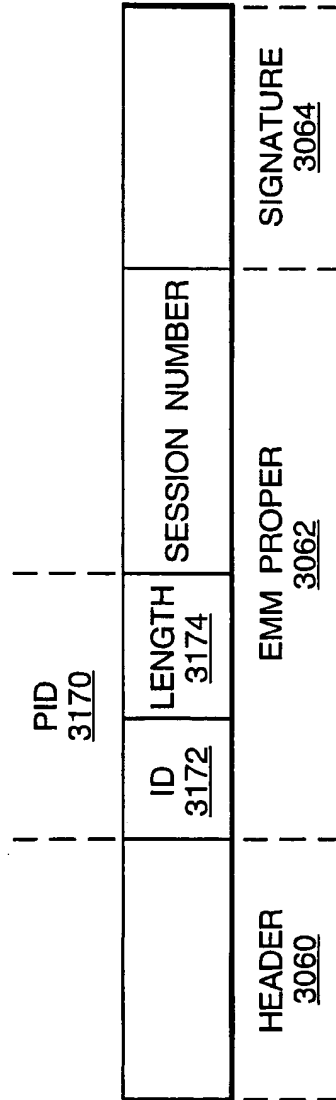
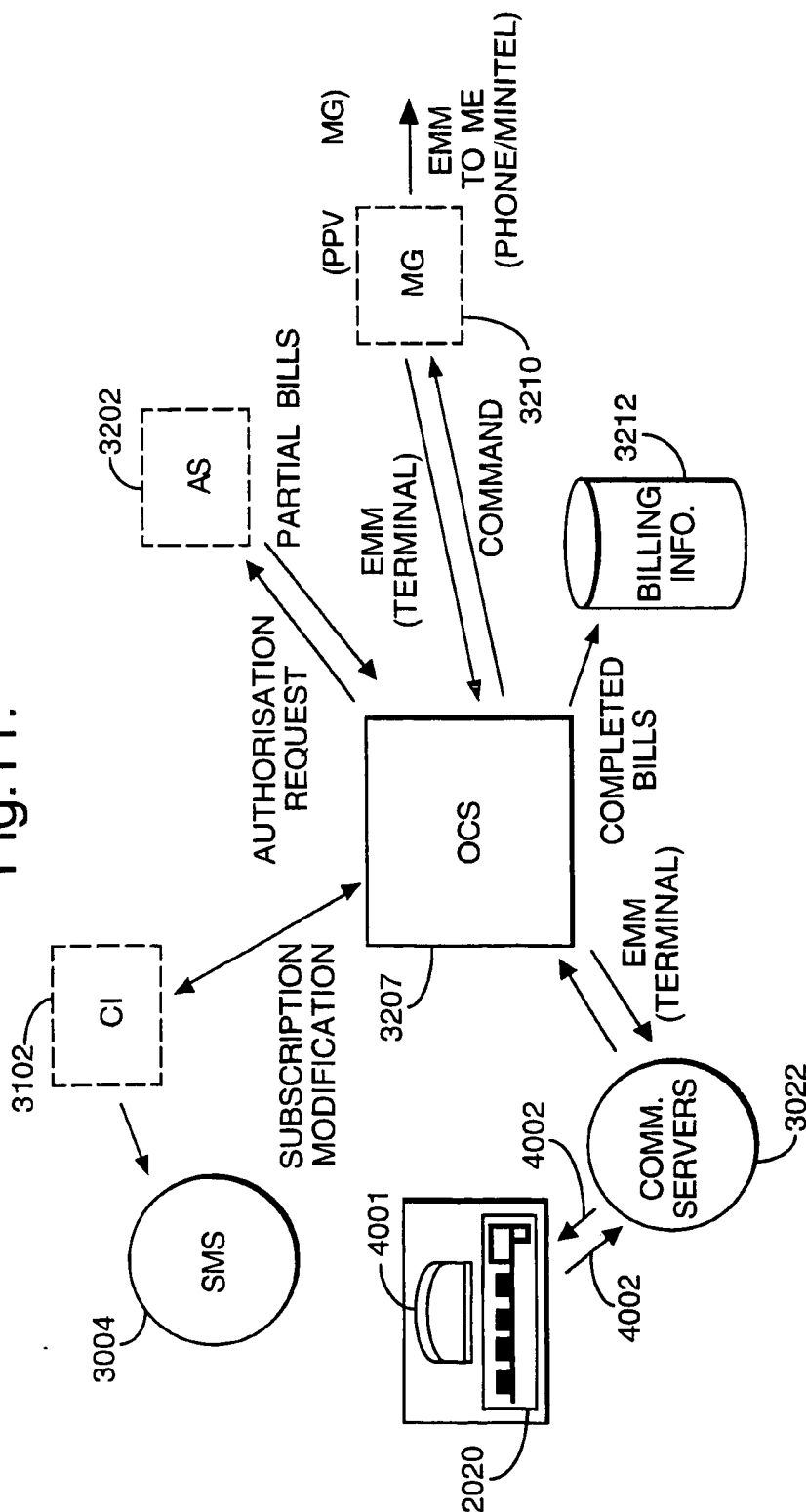


Fig.10.



9/17

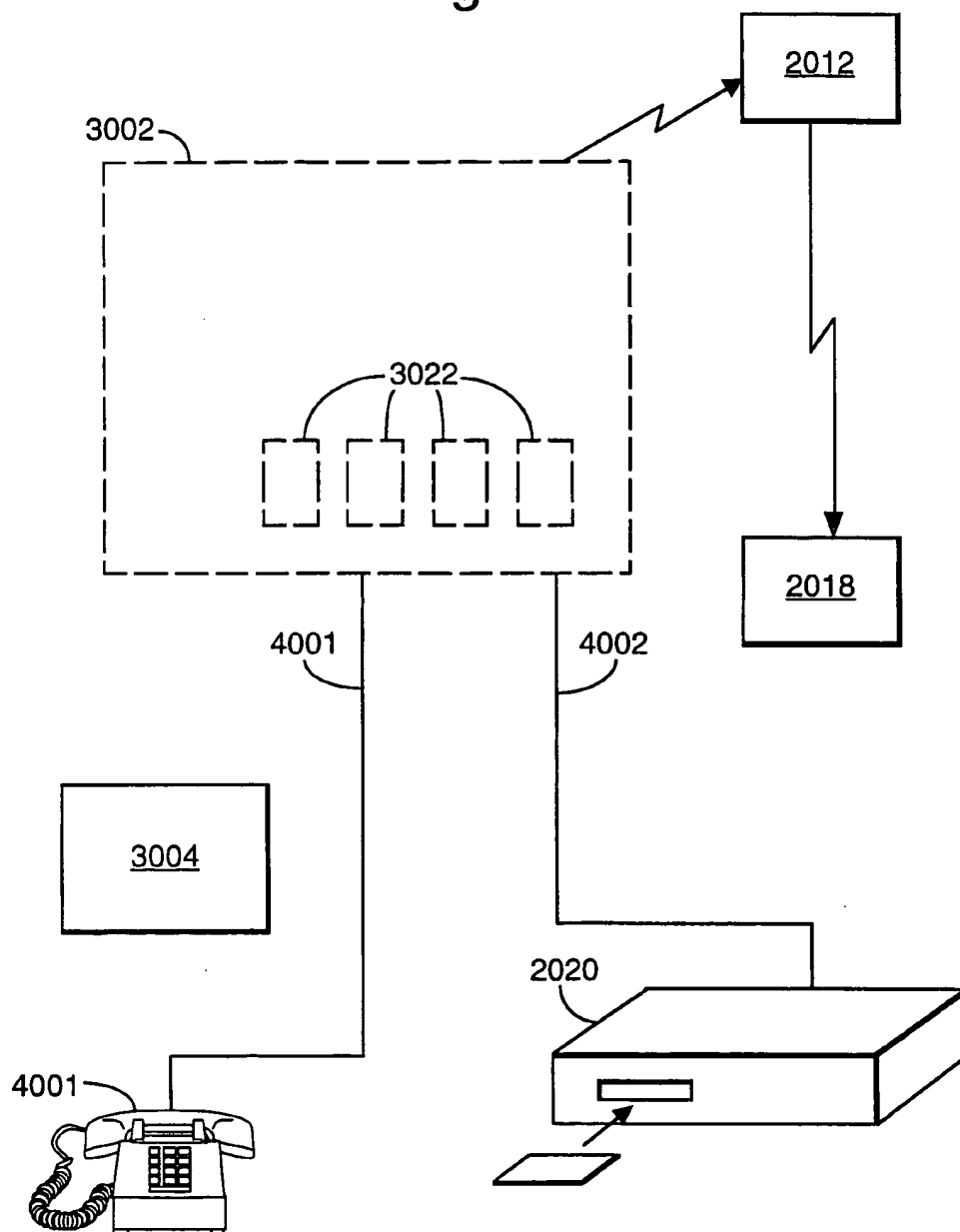
Fig. 11.



SUBSTITUTE SHEET (RULE 26)

10/17

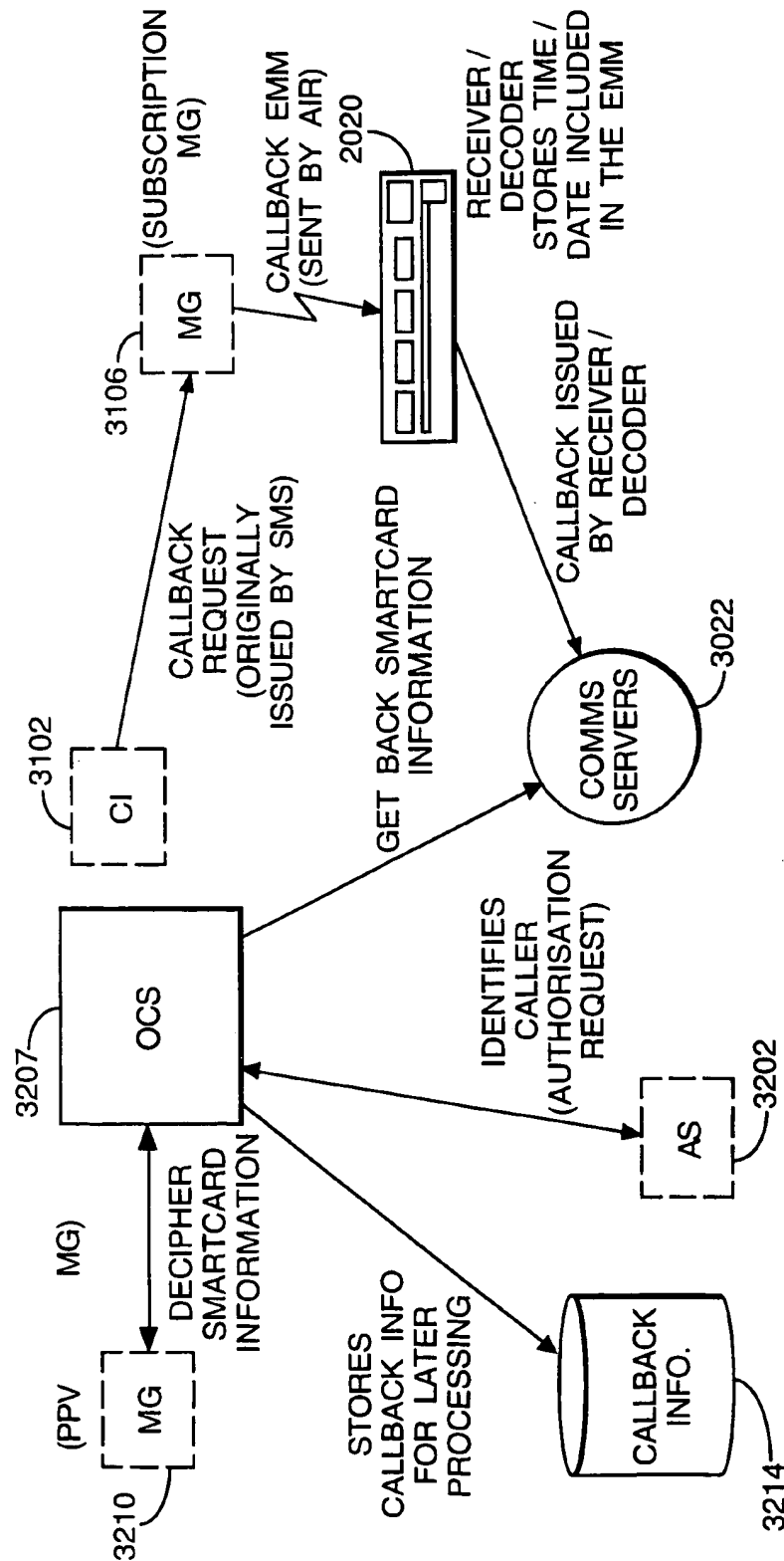
Fig.12.



SUBSTITUTE SHEET (RULE 26)

11/17

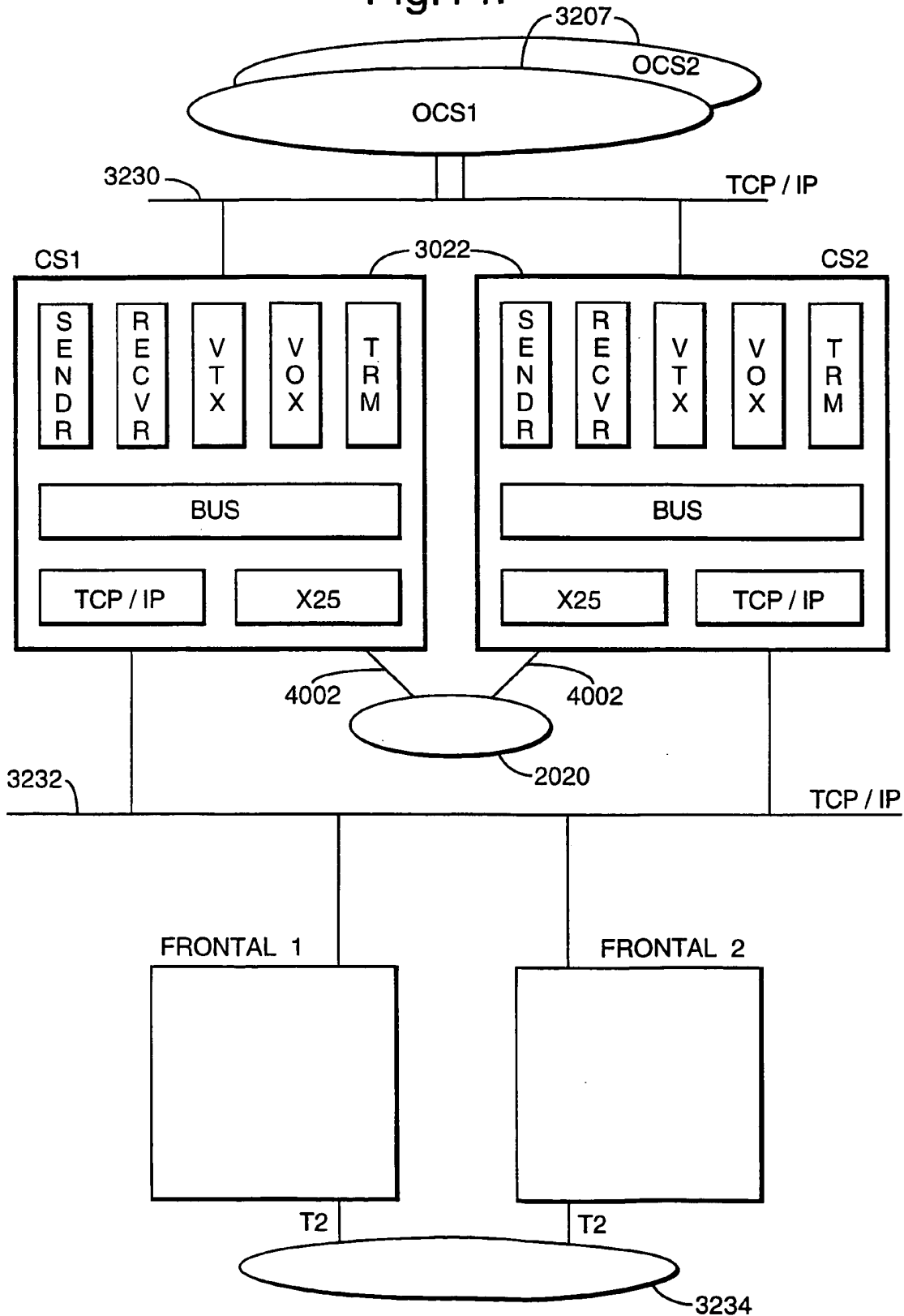
Fig.13.



SUBSTITUTE SHEET (RULE 26)

12/17

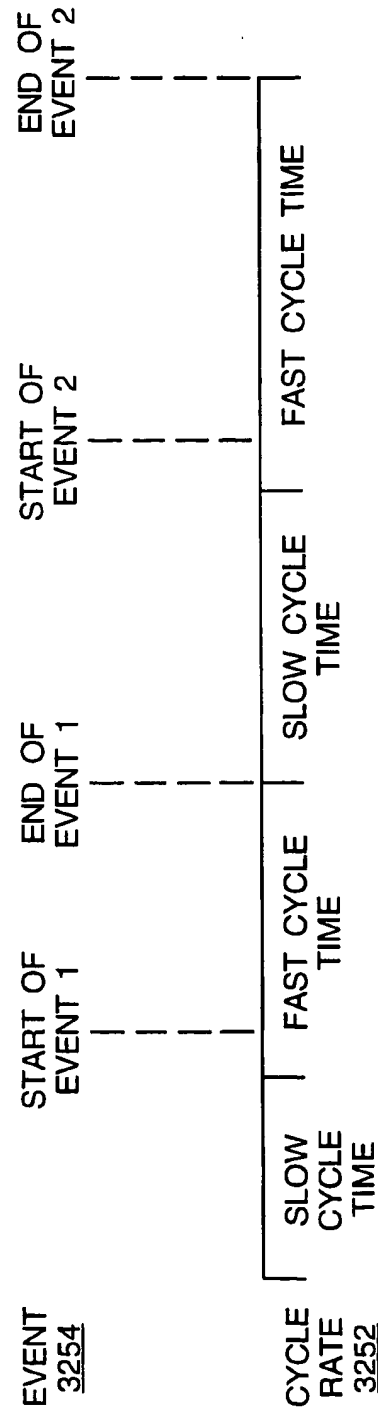
Fig.14.



SUBSTITUTE SHEET (RULE 26)

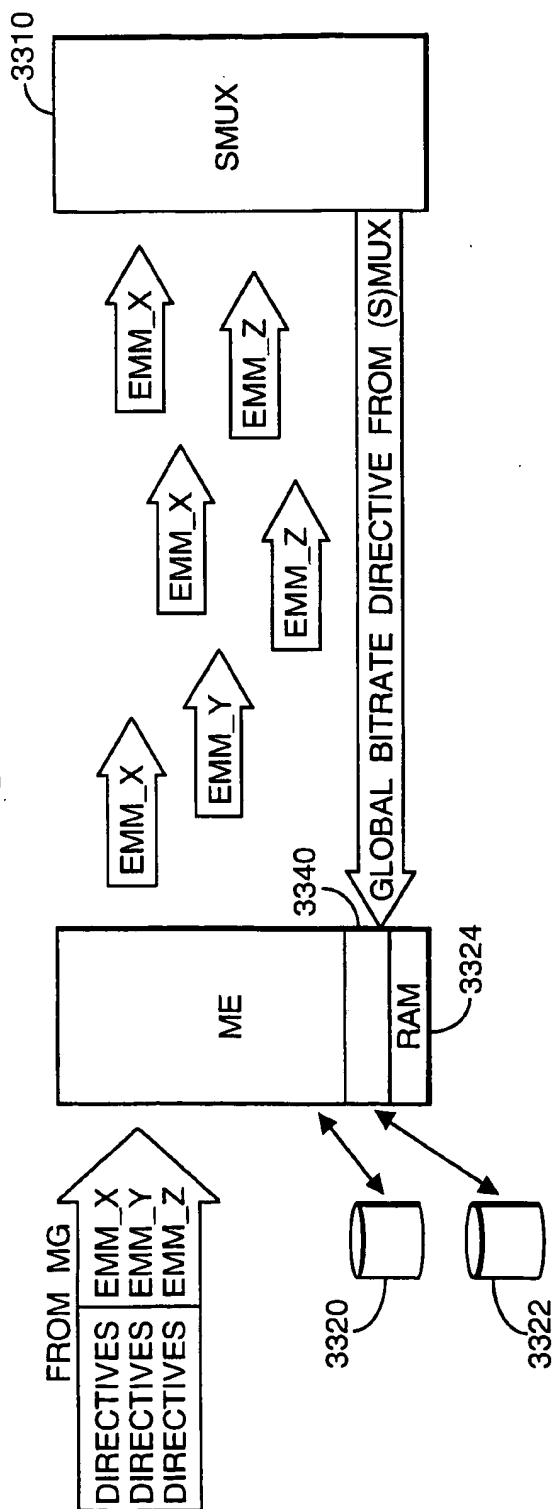
13/17

Fig.15.



SUBSTITUTE SHEET (RULE 26)

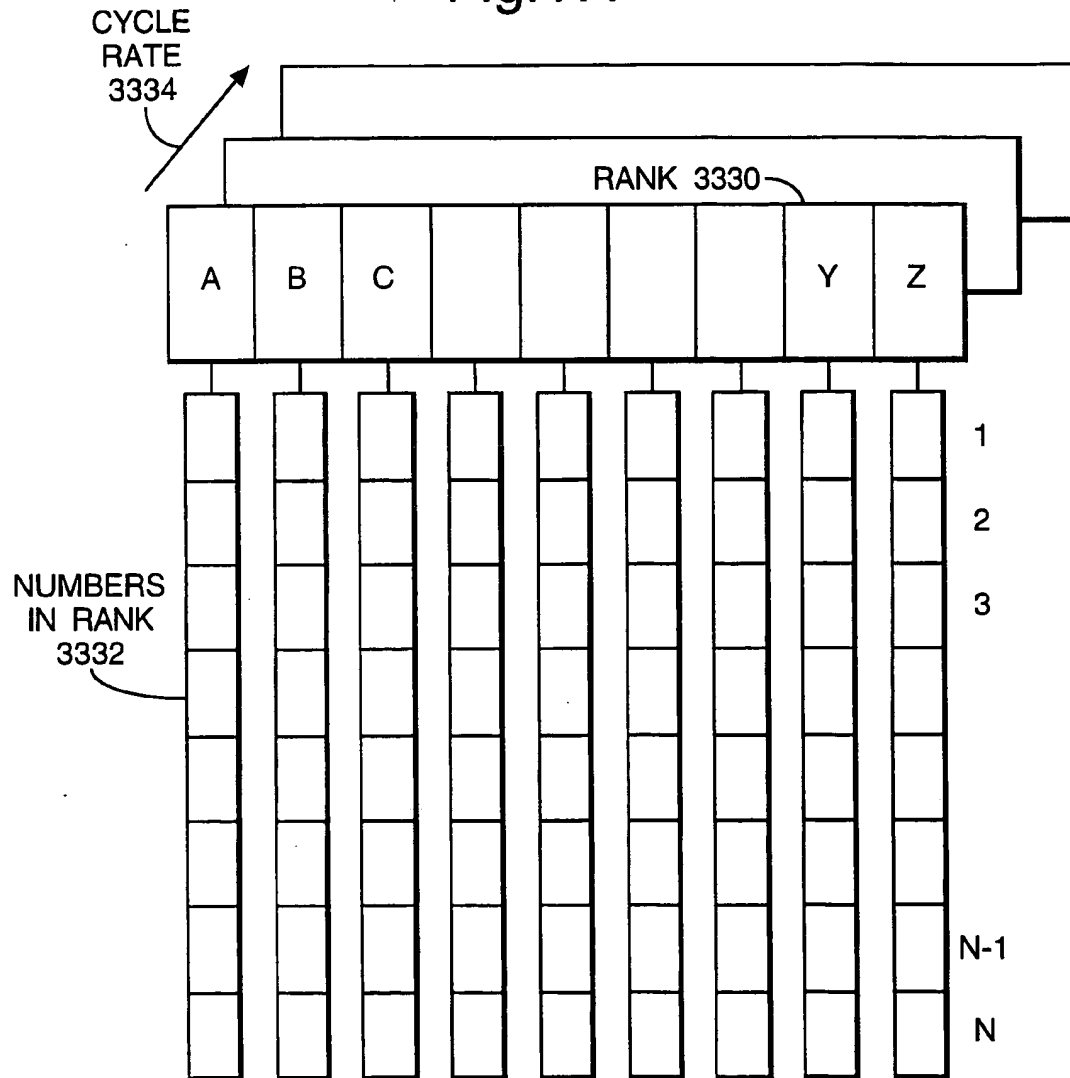
Fig.16.



SUBSTITUTE SHEET (RULE 26)

15/17

Fig.17.



SUBSTITUTE SHEET (RULE 26)

Fig.18.

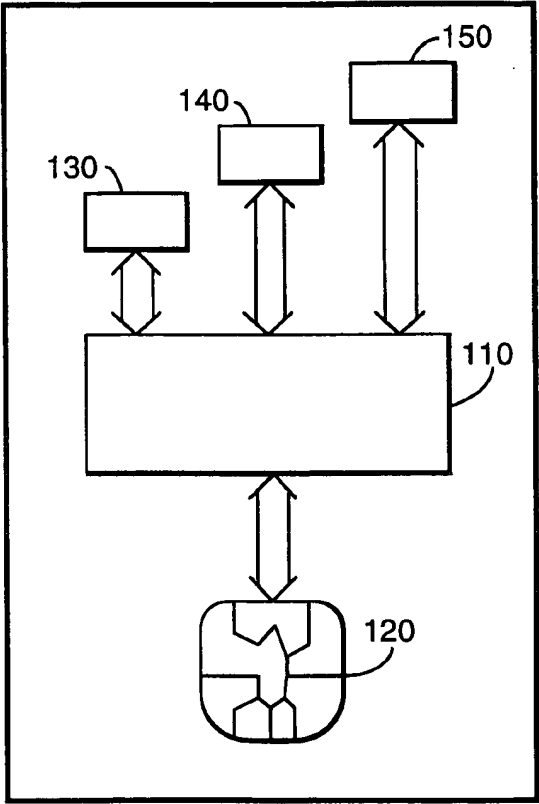
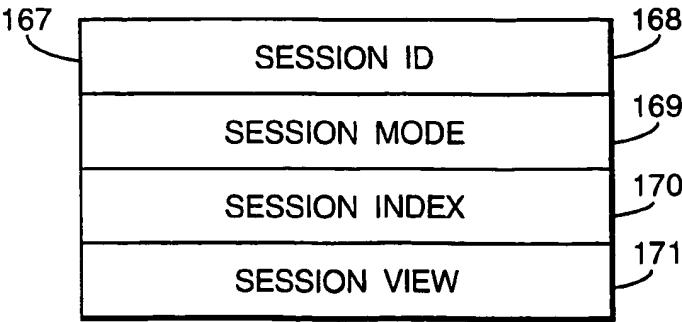


Fig.20.



SUBSTITUTE SHEET (RULE 26)

17/17

Fig.19.

CARD ID ZONE			151
RANDOM GEN. ZONE			152
MANAGEMENT ZONE			153
OPERATOR 1 ID			154
OPERATOR 2 ID			155
OPERATOR N ID			156
1	EMM KEY	DATA	157
1	ECM KEY	DATA	159
2	EMM KEY	DATA	
1	SUBS BITMAP	DATA	161
0	OBJECT FREE		166
3	ECM KEY	DATA	
1	TOKEN WALLET	DATA	163
1	PPV EVENT	DATA	165
N	ECM KEY	DATA	

SUBSTITUTE SHEET (RULE 26)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 97/02108

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, no. 266, 21 December 1995, pages 64-77, XP000559450 see the whole document ---	1-12, 15-19, 21,22
X	WO 94 14284 A (DISCOVERY COMMUNICAT INC) 23 June 1994 see page 8, line 8 - page 14, line 23 see page 18, line 28 - page 21, line 19 see page 24, line 25 - page 29, line 31 see page 33, line 8 - line 17 see figures 1-11 --- -/-	1-12, 14-17

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- * & * document member of the same patent family

Date of the actual completion of the international search

11 November 1997

Date of mailing of the international search report

18. 11. 97

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Van der Zaal, R

INTERNATIONAL SEARCH REPORT

Internat. Application No
PCT/EP 97/02108

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>US 5 144 663 A (KUDELSKI ANDRE ET AL) 1 September 1992 see column 2, line 5 - line 23 see column 3, line 6 - column 4, line 65 see column 5, line 62 - column 8, line 58 see figures 1-11 -----</p>	1-12

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No

PCT/EP 97/02108

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9414284 A	23-06-94	AU 5732994 A	04-07-94
		AU 5733094 A	04-07-94
		AU 5733194 A	04-07-94
		AU 5733294 A	04-07-94
		AU 5736394 A	04-07-94
		AU 5845894 A	22-06-94
		AU 5869894 A	04-07-94
		CA 2151458 A	23-06-94
		CN 1093211 A	05-10-94
		CN 1090451 A	03-08-94
		CN 1090452 A	03-08-94
		CN 1096151 A	07-12-94
		CN 1090453 A	03-08-94
		CN 1090454 A	03-08-94
		EP 0673578 A	27-09-95
		EP 0673579 A	27-09-95
		EP 0673580 A	27-09-95
		EP 0673581 A	27-09-95
		EP 0673582 A	27-09-95
		EP 0673583 A	27-09-95
		EP 0674824 A	04-10-95
		IL 107908 A	10-01-97
		IL 107909 A	15-04-97
		IL 107910 A	10-06-97
		IL 107912 A	18-02-97
		IL 107913 A	15-04-97
		JP 8510869 T	12-11-96
		JP 8506938 T	23-07-96
		JP 8506939 T	23-07-96
		JP 8506940 T	23-07-96
		JP 8506941 T	23-07-96
		JP 8506942 T	23-07-96
		NZ 259146 A	26-05-97
		NZ 259147 A	26-05-97
		NZ 259148 A	26-11-96
		WO 9413107 A	09-06-94
		WO 9414279 A	23-06-94
		WO 9414280 A	23-06-94
		WO 9414281 A	23-06-94
		WO 9414282 A	23-06-94

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 97/02108

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9414284 A		WO 9414283 A	23-06-94
		US 5559549 A	24-09-96
		US 5600364 A	04-02-97
		US 5659350 A	19-08-97

US 5144663 A	01-09-92	AU 599646 B	26-07-90
		AU 7157887 A	22-10-87
		DE 3751410 D	24-08-95
		DE 3751410 T	11-04-96
		EP 0243312 A	28-10-87
		EP 0626793 A	30-11-94
		ES 2076931 T	16-11-95
		JP 2610260 B	14-05-97
		JP 63023488 A	30-01-88
		JP 2520217 B	31-07-96
		JP 5244591 A	21-09-93

**NOTICE OF OFFICE PLAN TO CEASE SUPPLYING COPIES OF CITED U.S. PATENT
REFERENCES WITH OFFICE ACTIONS, AND PILOT TO EVALUATE THE
ALTERNATIVE OF PROVIDING ELECTRONIC ACCESS TO SUCH U.S. PATENT
REFERENCES**

Summary

The United States Patent and Trademark Office (Office or USPTO) plans in the near future to: (1) cease mailing copies of U.S. patents and U.S. patent application publications (US patent references) with Office actions except for citations made during the international stage of an international application under the Patent Cooperation Treaty and those made during reexamination proceedings; and (2) provide electronic access to, with convenient downloading capability of, the US patent references cited in an Office action via the Office's private Patent Application Information Retrieval (PAIR) system which has a new feature called "E-Patent Reference." Before ceasing to provide copies of U.S. patent references with Office actions, the Office shall test the feasibility of the E-Patent Reference feature by conducting a two-month pilot project starting with Office actions mailed after December 1, 2003. The Office shall evaluate the pilot project and publish the results in a notice which will be posted on the Office's web site (www.USPTO.gov) and in the Patent Official Gazette (O.G.). In order to use the new E-Patent Reference feature during the pilot period, or when the Office ceases to send copies of U.S. patent references with Office actions, the applicant must: (1) obtain a digital certificate from the Office; (2) obtain a customer number from the Office, and (3) properly associate applications with the customer number. The pilot project does not involve or affect the current Office practice of supplying paper copies of foreign patent documents and non-patent literature with Office actions. Paper copies of references will continue to be provided by the USPTO for searches and written opinions prepared by the USPTO for international applications during the international stage and for reexamination proceedings.

Description of Pilot Project to Provide Electronic Access to Cited U.S. Patent References

On December 1, 2003, the Office will make available a new feature, E-Patent Reference, in the Office's private PAIR system, to allow more convenient downloading of U.S. patents and U.S. patent application publications. The new feature will allow an authorized user of private PAIR to download some or all of the U.S. patents and U.S. patent application publications cited by an examiner on form PTO-892 in Office actions, as well as U.S. patents and U.S. patent application publications submitted by applicants on form PTO/SB08 (1449) as part of an IDS. The retrieval of some or all of the documents may be performed in one downloading step with the documents encoded as Adobe Portable Document format (.pdf) files, which is an improvement over the current page-by-page retrieval capability from other USPTO systems.

Steps to Use the New E-Patent Reference Feature During the Pilot Project and Thereafter

Access to private PAIR is required to utilize E-Patent Reference. If you don't already have access to private PAIR, the Office urges practitioners, and applicants not represented by a practitioner, to take advantage of the transition period to obtain a no-cost USPTO Public Key Infrastructure (PKI) digital certificate, obtain a USPTO customer number, associate all of their pending and new application filings with their customer number, install no-cost software (supplied by the Office) required to access private PAIR and E-Patent Reference feature, and make appropriate arrangements for Internet access. The full instructions for obtaining a PKI digital certificate are available at the Office's Electronic Business Center (EBC) web page at: <http://www.uspto.gov/ebc/downloads.html>. Note that a notarized signature will be required to obtain a digital certificate.

To get a Customer Number, download and complete the Customer Number Request form, PTO-SB125, at: <http://www.uspto.gov/web/forms/sb0125.pdf>. The completed form can then be transmitted by facsimile to the Electronic Business Center at (703) 308-2840, or mailed to the address on the form. If you are a registered attorney or patent agent, then your registration number must be associated with your customer number. This is accomplished by adding your registration number to the Customer Number Request form. A description of associating a customer number with an application is described at the EBC web page at: http://www.uspto.gov/ebc/registration_pair.html.

The E-Patent Reference feature will be accessed using a new button on the private PAIR screen. Ordinarily all of the cited U.S. patent and U.S. patent application publication references will be available over the Internet using the Office's new E-Patent Reference feature. The size of the references to be downloaded will be displayed by E-Patent Reference so the download time can be estimated. Applicants and registered practitioners can select to download all of the references or any combination of cited references. Selected references will be downloaded as complete documents as Adobe Portable Document Format (.pdf) files. For a limited period of time, the USPTO will include a copy of this notice with Office actions to encourage applicants to use this new feature and, if needed, to take the steps outlined above in order to be able to utilize this new feature during the pilot and thereafter.

During the two-month pilot, the Office will evaluate the stability and capacity of the E-Patent Reference feature to reliably provide electronic access to cited U.S. patent and U.S. patent application publication references. While copies of U.S. patent and U.S. patent application publication references cited by examiners will continue to be mailed with Office actions during the pilot project, applicants are encouraged to use the private PAIR and the E-Patent Reference feature to electronically access and download cited U.S. patent and U.S. patent application publication references so the Office will be able to objectively evaluate its performance. The public is encouraged to submit comments to the Office on the usability and performance of the E-Patent Reference feature during the pilot. Further, during the pilot period registered practitioners, and applicants not represented by a practitioner, are encouraged to experiment with the feature, develop a proficiency in using the feature, and establish new internal processes for using the new access to the cited U.S. patents and U.S. patent application publications to prepare for the anticipated cessation of the current Office practice of supplying copies of such cited

references. The Office plans to continue to provide access to the E-Patent Reference feature during its evaluation of the pilot.

Comments

Comments concerning the E-Patent Reference feature should be in writing and directed to the Electronic Business Center (EBC) at the USPTO by electronic mail at eReference@uspto.gov or by facsimile to (703) 308-2840. Comments will be posted and made available for public inspection. To ensure that comments are considered in the evaluation of the pilot project, comments should be submitted in writing by January 15, 2004.

Comments with respect to specific applications should be sent to the Technology Centers' customer service centers. Comments concerning digital certificates, customer numbers, and associating customer numbers with applications should be sent to the Electronic Business Center (EBC) at the USPTO by facsimile at (703) 308-2840 or by e-mail at EBC@uspto.gov.

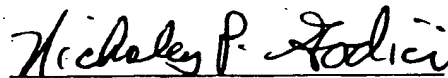
Implementation after Pilot

After the pilot, its evaluation, and publication of a subsequent notice as indicated above, the Office expects to implement its plan to cease mailing paper copies of U.S. patent references cited during examination of non provisional applications on or after February 2, 2004; although copies of cited foreign patent documents, as well as non-patent literature, will still be mailed to the applicant until such time as substantially all applications have been scanned into IFW.

For Further Information Contact

Technical information on the operation of the IFW system can be found on the USPTO website at <http://www.uspto.gov/web/patents/ifw/index.html>. Comments concerning the E-Patent Reference feature and questions concerning the operation of the PAIR system should be directed to the EBC at the USPTO at (866) 217-9197. The EBC may also be contacted by facsimile at (703) 308-2840 or by e-mail at EBC@uspto.gov.

Date. 12/1/03



Nicholas P. Godici
Commissioner for Patents

USPTO TO PROVIDE ELECTRONIC ACCESS TO CITED U.S. PATENT REFERENCES WITH OFFICE ACTIONS AND CEASE SUPPLYING PAPER COPIES

In support of its 21st Century Strategic Plan goal of increased patent e-Government, beginning in June 2004, the United States Patent and Trademark Office (Office or USPTO) will begin the phase-in of its E-Patent Reference program and hence will: (1) **provide downloading capability of the U.S. patents and U.S. patent application publications cited in Office actions** via the E-Patent Reference feature of the Office's Patent Application Information Retrieval (PAIR) system; and (2) **cease mailing paper copies of U.S. patents and U.S. patent application publications with Office actions** (in applications and during reexamination proceedings) except for citations made during the international stage of an international application under the Patent Cooperation Treaty (PCT). In order to use the new E-Patent Reference feature applicants must: (1) obtain a digital certificate and software from the Office; (2) obtain a customer number from the Office; and (3) properly associate patent applications with the customer number. Alternatively, copies of all U.S. patents and patent application publications can be accessed without a digital certificate from the USPTO web site, from the USPTO Office of Public Records, and from commercial sources. The Office will continue the practice of supplying paper copies of foreign patent documents and non-patent literature with Office actions. Paper copies of cited references will continue to be provided by the USPTO for international applications during the international stage.

Schedule

June 2004	TCs 1600, 1700, 2800 and 2900
July 2004	TCs 3600 and 3700
August 2004	TCs 2100 and 2600

All U.S. patents and U.S. patent application publications are available on the USPTO web site. However, a simple system for downloading the cited U.S. patents and patent application publications has been established for applicants, called the E-Patent Reference system. As E-Patent Reference and Private PAIR require participating applicants to have a customer number, retrieval software and a digital certificate, all applicants are strongly encouraged to contact the Patent Electronic Business Center to acquire these items. To be ready to use this system by June 1, 2004, contact the Patent EBC as soon as possible by phone at 866-217-9197 (toll-free), 703-305-3028 or 703-308-6845 or electronically via the Internet at ebc@uspto.gov.

Other Options

The E-Patent Reference function requires the applicant to use the secure Private PAIR system, which establishes confidential communications with the applicant. Applicants using this facility must receive a digital certificate, as described above. Other options for obtaining patents which do not require the digital certificate include the USPTO's free Patents on the Web program (<http://www.uspto.gov/patft/index.html>). The USPTO's Office of Public Records also supplies copies of patents for a fee (<http://ebiz1.uspto.gov/oems25p/index.html>). Commercial sources also provide U.S. patents and patent application publications.

For complete instructions see the Official Gazette Notice, USPTO TO PROVIDE ELECTRONIC ACCESS TO CITED U.S. PATENT REFERENCES WITH OFFICE ACTIONS AND CEASE SUPPLYING PAPER COPIES, on the USPTO web site.